INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Combinatorial Designs and Availability

Alain Jean-Marie — Xavier Roche — Vincent Boudet — Anne-Elisabeth Baert

N° 7119

December 2009

Thème COM

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--7119--FR+ENG

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

INRIA

centre de recherche
SOPHIA ANTIPOLIS - MÉDITERRANÉE

Combinatorial Designs and Availability

Alain Jean-Marie*, Xavier Roche†, Vincent Boudet†, Anne-Elisabeth Baert†

Thème COM — Systèmes communicants
Équipe-Projet Maestro

Rapport de recherche n° 7119 — December 2009 — 42 pages

Abstract: We consider a variation of Design Theory, in which the elements of the base set may be "available" or not. The random variable of interest is the number of subsets in the design which contain some available element. We are particularly interested in the variance of this variable, and we look for arrangements which minimize this value. We provide the solution to some instances of this problem; we show in particular that Steiner systems optimize this function.

Key-words: Combinatorial Designs, Steiner Systems, Round-Robin Tournaments

* INRIA and LIRMM, CNRS/Université Montpellier 2, 161 Rue Ada, F-34392 Montpellier, ajm@lirmm.fr.

† LIRMM, CNRS/Université Montpellier 2, 161 Rue Ada, F-34392 Montpellier, roche, boudet, baert@lirmm.fr.

Centre de recherche INRIA Sophia Antipolis – Méditerranée
2004, route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex
Téléphone : +33 4 92 38 77 77 — Télécopie : +33 4 92 38 77 65

Sur la mesure de disponibilité pour les arrangements combinatoires

Résumé : Nous considérons une variation en théorie des arrangements combinatoires, dans laquelle les éléments de l'ensemble de base peuvent être « disponibles » ou non. La variable aléatoire qui nous intéresse est le nombre de ces arrangements qui ont au moins un élément disponible. En particulier, nous nous intéressons à sa variance, et nous cherchons les arrangements qui la minimisent. Nous donnons la solution à certaines instances de ce problème; nous montrons en particulier que les Systèmes de Steiner optimisent cette métrique.

Mots-clés : Arrangements combinatoires, Systèmes de Steiner, Tournois

1 Introduction

We study in this report a probabilistic variation of Design Theory. Consider some set $\mathcal{V}$, the elements of which may be either "available" or not. Given a collection $\mathcal{B}$ of subsets of $\mathcal{V}$, we say that a subset is "available" if some element in it is itself available. A natural metric for the collection $\mathcal{V}$ is the number Λ of available subsets. Under simple probabilistic assumptions on individual availability, this is a random variable. Most of the present report is devoted to finding collections which minimize the variance of this random variable.

Possible interpretations and use for this construction are as follows. In the context of distributed systems, data is commonly replicated on several "servers". The set $\mathcal{V}$ represents the possible servers, and each subset represents the locations where a particular piece of data is replicated. If each server may be either available (or "online" in the networking jargon) or unavailable (*i.e.* offline), there is a risk that some piece of data be unreachable, despite the duplication. The random variable Λ is the number of pieces of data that are available, on at least one online server.

In the original interpretation of Design Theory, the subsets of $\mathcal{V}$ represent experiments with several products. Assuming that one experiment fails as soon as one of the products involved in it fails, then we count with Λ the number of failed experiments. Similar interpretations can be imagined in reliability theory, given a set $\mathcal{V}$ of elementary components or tasks, subject to individual failure, which are involved in more complex tasks: the elements of $\mathcal{B}$.

The report is organized as follows. In Section 2, we introduce formally the question of "availability", and we establish expressions for the distribution, average and variance of the random variable Λ.

In Section 3, we define the MINVAR problem, and we establish preliminary facts about the objective function J which we seek to minimize.

In Section 4, we relate the MINVAR problem to, on the one hand, a simpler problem called MINNI, and on the other hand, to a well-known difficult problem: finding Steiner systems.

Section 5 is devoted to cases where we can solve exactly the MINVAR problem. It is shown there that Steiner systems do solve the problem. We also provide necessary optimality conditions, and a construction of solutions for specific values of the parameters.

Section 6 approaches the problem from the point of view of Algebraic Combinatorics. We show that the MINVAR problem can be formulated as a convex quadratic integer program.

Sections 7 and 8 are concerned with the construction of "approximate" solutions. Section 7 shows that it is possible to compute the statistics of the objective function J for simple families of random designs. Section 8 then discusses in more details the lower bounds that can be established on J.

Finally, Section 9 states a conjecture we propose on the solution of the MINVAR problem, and discusses what would be consequences of this conjecture.

2 Combinatorial designs and availability

This section is devoted to the setting of the combinatorial optimization problem.

Consider a set $\mathcal{V}$ of objects, with cardinal $V = |\mathcal{V}|$. Assume that each of these objects is in one of two states: "available" and "unavailable". We say that a subset of $\mathcal{V}$ is unavailable if *all* its elements are unavailable, and available otherwise.

Assume now that the state of availability of the object $p \in \mathcal{V}$ is described by a random variable: X_p. Let $X_p = 1$ if p is *unavailable*, and $X_p = 0$ otherwise. Denote:

$$\delta(p) \;=\; \mathbb{P}(X_p = 0)\;, \qquad \bar{\delta} \;=\; 1 - \delta(p) \;=\; \mathbb{P}(X_p = 1)\;.$$

The parameter $\delta(p)$ is the availability of the individual object p.

Finally, consider the collection of subsets of $\mathcal{V}$, indexed by some set $\mathcal{B}$ of cardinal $B = |\mathcal{B}|$, and denoted as: $\{L(b); b \in \mathcal{B}\}$. The elements of this collection[1] will be referred to as *blocks*. We are interested in the random variable Λ which counts the number of blocks that are available, or equivalently, in $\overline{\Lambda}$ which counts the blocks that are unavailable. We proceed with establishing general expressions for their distribution and their first moments.

Define the Bernoulli random variable

$$U_j \;=\; 1 \text{ iff the block } L(j) \text{ is unavailable } 0 \text{ otherwise.} \tag{1}$$

From the definition of availability, we have:

$$U_j \;=\; \prod_{k \in L(j)} X_k\;,$$

and on the other hand,

$$\overline{\Lambda} \;=\; \sum_{j \in \mathcal{B}} U_j \;=\; \sum_{j \in \mathcal{B}} \prod_{k \in L(j)} X_k \qquad \text{or:} \qquad \Lambda \;=\; B \;-\; \sum_{j \in \mathcal{B}} \prod_{k \in L(j)} X_k\;.$$

In order to obtain an expression for the probability generating function (PGF) of the distribution of Λ the following observations are useful. First, if $x \in \{0,1\}$, then $z^x = 1 - x + zx = 1 + x(z-1)$. Second, if $x_i \in \{0,1\}$ and A, B are two sets of indices, $\prod_{i \in A} x_i \prod_{j \in B} x_j = \prod_{i \in A \cup B} x_i$. It follows that:

$$\begin{aligned} z^{\overline{\Lambda}} &= \prod_{j \in \mathcal{B}} z^{\prod_{k \in L(j)} X_k} \;=\; \prod_{j \in \mathcal{B}} \left(1 + (z-1) \prod_{k \in L(j)} X_k \right) \\ &= \sum_{\mathcal{S} \subset \mathcal{B}} (z-1)^{|\mathcal{S}|} \prod_{p \in \cup_{j \in \mathcal{S}} L(j)} X_p\;. \end{aligned}$$

It follows that, assuming the independence of the random variables X_p, the PGF of $\overline{\Lambda}$ can be expressed as:

$$\mathbb{E}(z^{\overline{\Lambda}}) \;=\; \sum_{\mathcal{S} \subset \mathcal{B}} (z-1)^{|\mathcal{S}|} \prod_{p \in \cup_{j \in \mathcal{S}} L(j)} \bar{\delta}_p\;.$$

[1] Such collections are called "Set Systems" in [1] and "Incidence Structures" in [2].

We summarize in the following theorem the principal results on this distribution, for the special case of interest to us.

Theorem 1. *Assume that* $\delta(p) = \delta$ *for all* $p \in \mathcal{V}$. *Then the probability generating function of the number* $\overline{\Lambda}$ *of unavailable blocks is given by:*

$$\mathbb{E}(z^{\overline{\Lambda}}) \;=\; \sum_{\mathcal{S}\subset\mathcal{B}} (z-1)^{|\mathcal{S}|}\; \bar{\delta}^{|\cup_{j\in\mathcal{S}} L(j)|}\,. \tag{2}$$

Assume further that $|L(j)| = K$ *for all* $j \in \mathcal{B}$. *The first moments of* Λ *and* $\overline{\Lambda}$ *are given by:*

$$\begin{aligned}
\mathbb{E}(\overline{\Lambda}) &= B\,\bar{\delta}^K & (3)\\
\mathbb{E}(\Lambda) &= B\,(1-\bar{\delta}^K) & (4)\\
\mathbb{V}(\overline{\Lambda}) \;=\; \mathbb{V}(\Lambda) &= \sum_{j,j'} \left(\bar{\delta}^{|L(j)\cup L(j')|} \;-\; \bar{\delta}^{2K} \right)\,. & (5)
\end{aligned}$$

Proof. The expression (2) for the PGF results from the preliminary analysis. For the mean, we have directly from the definition of U_j and the independence of the X_k:

$$\mathbb{E}\,U_j \;=\; \prod_{k\in L(j)} \mathbb{E}(X_k) \;=\; \bar{\delta}^K\,.$$

The result follows from $\overline{\Lambda} = \sum_j U_j$, then $\Lambda = B - \overline{\Lambda}$.

For the variance, we have:

$$\mathbb{V}(\overline{\Lambda}) \;=\; \mathbb{V}(\Lambda) \;=\; \sum_{j=1}^{B} \mathbb{V}(U_j) + \sum_{k\neq j} \mathrm{Cov}(U_k, U_j)\,. \tag{6}$$

It is known that

$$\begin{aligned}
\mathrm{Cov}(U_k,U_j) &= \mathbb{E}(U_kU_j) - \mathbb{E}(U_k)\mathbb{E}(U_j)\\
&= \bar{\delta}^{|L(k)\cup L(j)|} - \bar{\delta}^{|L(k)|+|L(j)|}\,.\\
\mathbb{V}(U_j) &= \mathbb{E}({U_j}^2) - \mathbb{E}(U_j)^2\\
&= \bar{\delta}^{|L(j)|} - \bar{\delta}^{2|L(j)|}\,.
\end{aligned}$$

Replacing in (6), it follows that:

$$\mathbb{V}(\Lambda) \;=\; B\,(\bar{\delta}^K - \bar{\delta}^{2K}) \;+\; \sum_{k\neq j} (\bar{\delta}^{|L(k)\cup L(j)|} - \bar{\delta}^{2K})\,. \tag{7}$$

Hence the result. An alternative derivation follows from differentiating (2) twice with respect to z and evaluating at $z = 1$. □

As a consequence of this theorem, we know that the expected value of Λ *does not* depend on the particular collection of subsets $\{L(b); b \in \mathcal{B}\}$, whereas the variance and the distribution in general do depend on it. The remainder of this paper is devoted to the search for collections which minimize the variance of Λ.

3 The MINVAR Problem

In this section, we define the MINVAR problem and state elementary properties.

3.1 Statement of the problem

Starting from Eq. (7), using the fact that $|L(k) \cup L(j)| = |L(j)| + |L(k)| - |L(k) \cap L(j)|$, letting $\gamma = \bar{\delta}^{-1}$, and assuming that $|L(j)| = K$ for all j, we obtain the expression:

$$\mathbb{V}(\Lambda) \;=\; B(\gamma^{-K} - \gamma^{-2K}) \;+\; \gamma^{-2K} \sum_{k \neq j} \left(\gamma^{|L(k) \cap L(j)|} - 1 \right) \;.$$

Accordingly, minimizing (5) or (7) is equivalent to minimizing the following objective function :

$$\sum_{k \neq j} \gamma^{|L(k) \cap L(j)|} \;.$$

We formulate this problem in the language of graph theory. Given a bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$, where $\mathcal{B}$, $\mathcal{V}$ are sets of vertices and $\mathcal{E}$ the set of edges, we define the function:

$$J(\mathcal{G}, \gamma) = \sum_{b \neq b' \in \mathcal{B}} \gamma^{|L(b) \cap L(b')|} \,, \tag{8}$$

where $L(b)$ denote the neighborhood of b in the graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$.[2] Obviously, the problem does not depend on the nature of the sets $\mathcal{B}$ and $\mathcal{V}$ but only on their size.

Our problem is the following:

Definition 1. *We define the MINVAR(B, V, K, γ) optimization problem as finding one bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$ with $|\mathcal{B}| = B$ and $|\mathcal{V}| = V$, which minimizes the function $J(\mathcal{G}, \gamma)$ under constraints*

$$\forall b \in \mathcal{B}, \qquad |L(b)| = K \;. \tag{9}$$

3.2 Properties of the objective function

We discuss in this section elementary properties of the function J.

Interference Generating Function. Denote with ν_ℓ the number of *distinct* couples of blocks which have exactly ℓ neighbors in common:

$$\nu_\ell \;=\; \#\left\{ (b, b') \text{ s.t. } b \neq b' \text{ and } |L(b) \cap L(b')| = \ell \right\} \;. \tag{10}$$

Then we have:

$$J(\mathcal{G}, \gamma) \;=\; \sum_{\ell=0}^{K} \nu_\ell \, \gamma^\ell \;. \tag{11}$$

[2] The incidence matrix of the bipartite graph $\mathcal{G}$ is the incidence matrix of the incidence structure in the sense of [2]. We shall sometimes call "blocks" the neighborhoods of elements of $\mathcal{B}$, in accordance with the terminology of Design Theory.

We shall call "interferences" the elements of some $L(b) \cap L(b')$. Accordingly, we shall also refer to $J(\mathcal{G},\gamma)$ as the interference generating function, or interference function, for graph $\mathcal{G}$.

Degree. The interference function is a polynomial of degree at most K. Its exact degree is

$$\partial^o J(\mathcal{G},\gamma) \;=\; \max\{|L(b)\cap L(b')|, (b,b') \in \mathcal{B}\times\mathcal{B}, b \neq b'\} \;=\; \max\{\ell \mid \nu_\ell \neq 0\} \;.$$

Modified Generating Function. It is often more convenient to use the "modified polynomial" defined as:

$$\widetilde{J}(\mathcal{G},\gamma) \;=\; \sum_{b,b'} \gamma^{|L(b)\cap L(b')|} \;. \tag{12}$$

Obviously, $\widetilde{J}(\mathcal{G},\gamma) = J(\mathcal{G},\gamma) + B\gamma^K$, so that both polynomials are equivalent for optimization purposes. Although we could work with the more "natural" function $\widetilde{J}$ only, we shall keep the focus on J because its degree is an important parameter, whereas the degree of $\widetilde{J}$ is always K. The polynomial $\widetilde{J}$ is the generating function of the numbers:

$$\tilde{\nu}_\ell \;=\; \#\big\{(b,b') \text{ s.t. } |L(b)\cap L(b')| = \ell\big\} \;.$$

Special Values. The values $J(\mathcal{G},1) = B(B-1)$ and $\widetilde{J}(\mathcal{G},1) = B^2$ are independent from $\mathcal{G}$.

Moment Generating Functions. The Taylor expansion of J at $\gamma = 1$ will be of central importance in the following. We have:

$$J(\mathcal{G},\gamma) \;=\; \sum_{p=0}^{K} \mu_p\,(\gamma-1)^p \;, \tag{13}$$

where the coefficients μ_ℓ are:

$$\mu_p \;=\; \frac{1}{p!}\,\frac{\partial^p J}{\partial\gamma^p}(\mathcal{G},1) \;=\; \sum_{b\neq b'\in\mathcal{B}} \binom{|L(b)\cap L(b')|}{p} \;.$$

The μ_p are related to the ν_ℓ through the binomial expansions:

$$\mu_p \;=\; \sum_{\ell=p}^{K} \binom{\ell}{p}\nu_\ell \qquad \nu_\ell \;=\; \sum_{p=\ell}^{K} (-1)^{p-\ell}\binom{p}{\ell}\mu_p \;. \tag{14}$$

In particular, we have the following relationships:

$$\mu_0 \;=\; J(\mathcal{G},1) \;=\; B(B-1)$$

$$\mu_1 \;=\; \sum_{\ell=1}^{K} \ell\nu_\ell \;=\; \sum_{b\neq b'\in\mathcal{B}} |L(b)\cap L(b')| \tag{15}$$

$$\begin{aligned}\mu_2 \;&=\; \sum_{\ell=1}^{K} \frac{1}{2}\ell(\ell-1)\nu_\ell \;=\; \frac{1}{2}\sum_{b\neq b'\in\mathcal{B}} |L(b)\cap L(b')|(|L(b)\cap L(b')|-1)\\ &=\; \frac{1}{2}\left(\sum_{b\neq b'\in\mathcal{B}} |L(b)\cap L(b')|^2 \;-\; \mu_1\right) \;.\end{aligned} \tag{16}$$

Similar expressions hold for the Taylor expansion of $\widetilde{J}$ at $z = 1$, with the sums taken over all (b,b') instead of $b \neq b'$.

4 Related problems

The MINVAR problem has a real parameter $\gamma \geq 1$. In this section, we look at the two "extreme" cases: γ close to 1 and γ large. In the first case, the problem reduces to a much simpler problem which we solve (Section 4.2). In the other case, we show that the problem is related to finding Steiner systems (Section 4.3).

4.1 Extreme Cases of the MINVAR Problem

Observe that if $\gamma \sim 1$, then according to (13), $J(\mathcal{G},\gamma) \sim B(B-1) + (\gamma-1)\mu_1$ where $\mu_1 = \sum_{b \neq b' \in \mathcal{B}} |L(b) \cap L(b')|$. Then the MINVAR problem is (approximately) equivalent to minimizing the total number of what we have called interferences in Section 3.2. We shall consider this problem below. According to our conjecture, to be discussed in Section 9, every graph solving the MINVAR problem should also minimize the number of interferences. This is an additional motivation for analyzing this problem.

On the other hand, if $\gamma \gg 1$, then $J(\mathcal{G},\gamma) \sim a\gamma^{\max_{b \neq b'} |L(b) \cap L(b')|}$, where a is the number of pairs (b,b') which achieve the maximum. In that case, the MINVAR problem is (approximately) equivalent to minimizing the maximal interference and, as a secondary objective, minimize the number of interferences that are maximal. Steiner systems are precisely incidence structures in which interferences are minimal.

This problem is also related to the theory of codes. Indeed, consider a binary code on V bits, with $\mathcal{B}$ the set of codewords, and $\mathcal{V}$ the set of bits. Let $\mathcal{G}$ be the bipartite graph obtained by letting $L(b)$ be the set of bits of the codeword b that are set to 1. Then the Hamming distance between two codewords b and b' is $d(b,b') = |L(b)| + |L(b')| - |L(b) \cap L(b')|$. If the code is a *constant weight code* [3], then $d(b,b') = 2K - |L(b) \cap L(b')|$ and maximizing the minimal distance between codewords is equivalent to minimizing the maximal interference.

4.2 Stable graphs and the MINNI Problem

We have seen in the previous section that the MINVAR problem is related to the problem of minimizing interferences in a bipartite graph. This section is devoted to the analysis of this problem.

We first introduce the definition:

Definition 2 (Number of interferences)**.** *Given a bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$, we define the number of interferences $NI(\mathcal{G})$ as:*

$$NI(\mathcal{G}) = \sum_{b \neq b' \in \mathcal{B}} |L(b) \cap L(b')| \ . \tag{17}$$

The number of interferences $NI(\mathcal{G})$ is the coefficient μ_1 introduced in Section 3.2: $NI(\mathcal{G}) = \mu_1 = J'(\mathcal{G}, 1)$.

Definition 3. *We define the MINNI(B,V,K) optimization problem as finding one bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$ with $|\mathcal{B}| = B$ and $|\mathcal{V}| = V$, which minimizes the interference function $NI(\mathcal{G})$ under constraints*

$$\forall b \in \mathcal{B}\ |L(b)| = K\ .$$

We now introduce the notion of stability, which is linked to the optimization of the number of interferences, as stated in the following result.

Definition 4 (Stability)**.** *A bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$ is stable if and only if $\forall p \neq p' \in \mathcal{V}$ we have*

$$|\delta(p) - \delta(p')| < 2 \tag{18}$$

where $\delta(p)$ is the degree of p.

An equivalent definition is that there exists some integer r such that the *replication numbers* $\delta(p) \in \{r, r+1\}, \forall p \in \mathcal{V}$.[3]

Proposition 1. *Every stable graph $\mathcal{G}$ minimizes $NI(\mathcal{G})$ under the constraint*

$$\forall b \in \mathcal{B}, \qquad |L(b)| = K\ .$$

$\diamond$ *Proof*. First, write down the number of interferences in $\mathcal{G}$ as:

$$\begin{aligned} NI(\mathcal{G}) &= \sum_{b \neq b' \in \mathcal{B}} |L(b) \cap L(b')| \\ &= \sum_{b \neq b' \in \mathcal{B}} \sum_{p \in \mathcal{V}} \mathbf{1}_{b,p} \mathbf{1}_{b',p} \\ &= \sum_{p \in \mathcal{V}} \sum_{b \neq b' \in \mathcal{B}} \mathbf{1}_{b,p} \mathbf{1}_{b',p}\ . \end{aligned}$$

But $\sum_{b \neq b' \in \mathcal{B}} \mathbf{1}_{b,p} \mathbf{1}_{b',p}$ is the number of pairs of edges leaving p. So it is $\delta(p) \times (\delta(p) - 1)$. Therefore,

$$\begin{aligned} NI(\mathcal{G}) &= \sum_{p \in \mathcal{V}} \delta(p) \times (\delta(p) - 1) \\ &= \sum_{p \in \mathcal{V}} \delta(p)^2 - B \times K\ . \end{aligned}$$

The square function is convex and the minimum of $\sum_{p \in \mathcal{V}} \delta(p)^2$ under the constraint $\sum_{p \in \mathcal{V}} \delta(p) = B \times K$, is attained for values of $\delta(p) = \lfloor BK/V \rfloor$ or $\delta(p) = \lceil BK/V \rceil$.

More precisely, if BK/V is an integer, then $\delta(p) = BK/V$ minimizes the function above. If not, then $BK = Vr + q$ with $1 \leq q < V$, and any vector $(\delta(p))_p$ such that q values are equal to $r+1$ and $V - q$ equal to r minimizes the function.

Therefore, NI is minimal if and only if the graph is stable. □

[3] Accordingly, the notion of stability could be termed “quasi r-regularity”, see [1, p. 4].

To conclude this section, two observations.

First, it is always possible to construct, in polynomial time in B, K and V, a graph which is stable and therefore solves the MINNI problem.

For instance, starting from any graph with the constraint (9), the algorithm that moves the extremity of one edge from the highest-degree p to a node with a degree less by at least 2, converges in a finite number of steps to a stable graph.[4]

4.3 Steiner Systems and Steiner Graphs

In this section, we reduce the MINVAR problem to the existence of a Steiner system. See also Theorem 5 in Section 5.3.3 and and Corollary 3 in Section 8.2.

Definition 5 (Steiner Systems)**.** *A Steiner system $S(t,k,v)$ is a collection of k-subsets (also called blocks) of a v-set such that each t-tuple of elements of this v-set is contained in a unique block.*

It is known (see e.g. [3, p. 60]) that there are exactly exactly

$$\frac{v!(k-t)!}{k!(v-t)!} \tag{19}$$

subsets in a $S(t,k,v)$.

Since we have adopted the terminology of bipartite graphs, we also define the graph version of Steiner systems.

Definition 6 (Steiner Graphs)**.** *Assume that for some triple (t,k,v), there is a Steiner system $C = S(t,k,v)$. The Steiner Graph is the bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$ with: $\mathcal{B} = C$, $\mathcal{V} = \{1,\ldots,v\}$, and edges between $b \in C$ and $p \in \mathcal{V}$ if and only if $p \in b$.*

In other words, the neighborhood in $\mathcal{G}$ of each vertex $b \in C$ is the contents of b, considered as an element of C.

This graph has the parameters: $V = v$, $K = k$ and, according to (19),

$$B = \frac{V!(K-t)!}{K!(V-t)!} . \tag{20}$$

The Steiner problem is renowned for its difficulty. The algorithmic difficulty of finding a Steiner System with given parameters, or just deciding whether one exists, does not seem to be formalized in the literature. But for instance, no Steiner systems are known with t larger than 5 and only a few ones with $t = 5$ have been described [1, 3].

[4] See Lemma 1.8 and Theorem 1.9 of [2] for another use of this argument.

4.4 MINVAR Problem and Steiner Systems

We now connect the existence of solutions to certain instances of the MINVAR problem to the existence of Steiner Systems. This serves as certifying that the MINVAR problem is a difficult one. If there were an easy solution to it, there would be an easy way to construct Steiner systems, or disprove their existence. We shall prove later in Section 5.3 that Steiner Graphs do provide solutions to the MINVAR problem.

Proposition 2. *There exists a Steiner system $S(t,k,v)$ if and only if there is a solution $\mathcal{G}$ of the MINVAR(B,V,K,γ) problem with*

$$B = \frac{v!(k-t)!}{k!(v-t)!}, \qquad V = v, \qquad K = k,$$

and either:

i) $J(\mathcal{G},\gamma_0) < \gamma_0^t$, where $\gamma_0 = B(B-1)+1$; or

ii) the degree of the polynomial $J(\mathcal{G},\gamma)$ is strictly less than t.

◇ *Proof*. Assume that there is a Steiner system $S(t,k,v)$ and let $\mathcal{G}$ be the associated Steiner Graph. In this graph, each pair $(b,b') \in \mathcal{B}\times\mathcal{B}, b \neq b'$ shares at most $t-1$ neighbors, for if they had t elements in common, this t-set would be contained in two distinct elements of C: b and b', and C would not be a Steiner system.

Therefore, $|L(b)\cap L(b')| \leq t-1$ for all $b \neq b'$, and we have created a solution $\mathcal{G}$ to the MINVAR(B,V,K,γ) problem such that the degree of J is strictly less than t. Since, for $\gamma > 1$, $J(\mathcal{G},\gamma) \leq B(B-1)\gamma^{\partial^\circ J}$, we also have $J(\mathcal{G},\gamma_0) \leq B(B-1)\gamma_0^{t-1} < \gamma_0^t$ for the value of γ_0 specified in *ii*.

Conversely, assume that there is a solution $\mathcal{G} = (\mathcal{B},\mathcal{V},\mathcal{E})$ of the MINVAR problem with $B = |\mathcal{B}| = \frac{v!(k-t)!}{k!(v-t)!}$, $V = |\mathcal{V}| = v$, $K = k$, for some (t,k,v), $\gamma = B(B-1)+1$ and either *i*) or *ii*).

Consider the collection $C = \{L(b)|b \in \mathcal{B}\}$ of subsets of $\mathcal{V}$. Then each subset of $\mathcal{V}$ of size t is included in at most one element of C. Otherwise, there would exist $b \neq b'$ such that $|L(b)\cap L(b')| \geq t$ and $J(\mathcal{G},\gamma)$ would be of degree larger than t, or equivalently, *ii*) would not hold. Furthermore, counting the number of vertices in $\mathcal{G}$, and using the fact that

$$\frac{v!(k-t)!}{k!(v-t)!}\binom{k}{t} = \binom{v}{t},$$

one concludes that each subset of size t appears in some element of C. Therefore, the collection C is a $S(t,k,v)$ Steiner system. □

5 Optimality Conditions and Solved Cases

We have proved in the previous section that the MINVAR problem is hard to solve in general. In this section, we show that not all values of K need to be considered. We provide a sufficient optimality conditions and describe one application. Finally, we provide a solution to the problem for $K = 2$.

5.1 Symmetry in K

We prove in this section that the values of K can be restricted to $K \leq V/2$ without loss of generality.

Proposition 3. *If $\mathcal{G} = (B,V,E)$ is an optimal solution of the problem MINVAR(B,V,K,γ), then $\mathcal{G}' = (B,V,E^c)$ is an optimal solution of MINVAR$(B,V,V-K,\gamma)$. Furthermore:*

$$J(\mathcal{G}',\gamma) = \gamma^{V-2K} J(\mathcal{G},\gamma).$$

◇ *Proof* . It is obvious that $\mathcal{G}'$ is a solution of MINVAR$(B,V,V-K,\gamma)$: it is a bipartite graph, where each vertex of $\mathcal{B}$ has exactly $V-K$ neighbors in V. Furthermore:

$$J(\mathcal{G}') = \sum_{b \neq b' \in \mathcal{B}} \gamma^{|L^c(b) \cap L^c(b')|}$$

$|L^c(b) \cap L^c(b')| = V + |L(b) \cap L(b')| - |L(b)| - |L(b')|$, then

$$\begin{aligned} J(\mathcal{G}') &= \gamma^{V-2K} \sum_{b \neq b' \in \mathcal{B}} \gamma^{|L(b) \cap L(b')|} \\ &= \gamma^{V-2K} J(\mathcal{G}) \end{aligned}$$

So, if $\mathcal{G}$ is an optimal solution of MINVAR(B,V,K,γ), $\mathcal{G}'$ is an optimal solution of MINVAR$(B,V,V-K,\gamma)$. □

As a consequence, we can assume $K \leq V/2$ if needed in the rest of the analysis.

5.2 Optimality Conditions

The topic of this paragraph is the presentation of a sufficient condition for optimality for the MINVAR problem. Recall the notion of stability (Definition 4) and introduce the notion of *uniformity* for bipartite graphs.

Definition 7 (Uniformity)**.** *A bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$ is uniform if and only if $\forall b \neq b' \in \mathcal{B}$ and $\forall c \neq c' \in \mathcal{B}$,*

$$||L(b) \cap L(b')| - |L(c) \cap L(c')|| < 2. \tag{21}$$

An equivalent definition is that there exists some integer μ such that the *intersection numbers* $|L(b) \cap L(b')| \in \{\mu, \mu+1\}$, $\forall b \neq b' \in \mathcal{B}$.[5]

Proposition 4. *If a graph $\mathcal{G}$ is stable and uniform, then it is a solution of MINVAR(B, V, K, γ), for any value of $\gamma \geq 1$.*

In the proof of this property, we shall use the following terminology:

Definition 8 (Assignation)**.** *We call s-assignation a series of $B(B-1)$ integers whose sum is equal to s.*

Each integer of an assignation (see Definition 8) may represent a value of $|L(b) \cap L(b')|$, for $(b, b') \in B, b \neq b'$. So, to each graph $\mathcal{G}$ corresponds an assignation of $NI(\mathcal{G})$ interferences, but some s-assignations do not match the list of interferences of any graph. Conversely, the definition of the function J depends on the graph $\mathcal{G}$ only through its sequence of numbers $|N(b) \cap N(b')|$, which is an assignation. Accordingly, we consider that J can be extended to be a function on assignations.

◇ *Proof of Proposition 4.* Let $\mathcal{G}_0$ be a stable and uniform graph, candidate solution to MINVAR(B, V, K, γ). As $\mathcal{G}_0$ is stable, Proposition 1 implies that $NI(\mathcal{G}_0) = N_0$ is minimal.

We define for any integer N:

- $\mathcal{D}_N$ the set of N-assignations.
- $\mathcal{C}_N$ the set of N-assignations that are produced by some bipartite graph $\mathcal{G}$ with parameters B and V, such that $|L(b)| = K$ for all $b \in \mathcal{B}$ and $NI(\mathcal{G}) = N$.
- d_N^* the N-assignation that minimizes J among $\mathcal{D}_N$.
- $A_{\mathcal{G}_0}$ the N-assignation produced by $\mathcal{G}_0$.

We have

$$\forall N : \mathcal{C}_N \subset \mathcal{D}_N$$

and

$$\forall N_1 \leq N_2, \quad J(d_{N_1}^*) \leq J(d_{N_2}^*).$$

With N_0 minimal, we obtain:

$$\forall \mathcal{G} : J(\mathcal{G}) \geq J(d_{N_0}^*) \ .$$

Now we prove that the N-assignations that minimize J among $\mathcal{D}_N$ are the uniform N-assignations. Assume by contradiction that some N-assignation A minimizes J among $\mathcal{D}_N$ and is not uniform:

$$\exists b \neq b' \in B, \quad \exists c \neq c' \in B, \quad A(b, b') - A(c, c') > 1 \ .$$

Then we define $A' \in \mathcal{D}_N$ as A, except:

[5] Accordingly, the notion of uniformity could be termed “quasi equidistance, see [1, p. 4].

- $A'(b,b') = A(b,b') - 1$
- $A'(c,c') = A(c,c') + 1$

For this new assignation, we have for every $\gamma \geq 1$:

$$\begin{array}{rcl} J(A') - J(A) & = & \gamma^{A(b,b')-1} - \gamma^{A(b,b')} + \gamma^{A(c,c')+1} - \gamma^{A(c,c')} \\ & = & (\gamma - 1)(\gamma^{A(c,c')} - \gamma^{A(b,b')-1}) \\ & < & 0 \,. \end{array}$$

So A does not minimize J among $\mathcal{D}_N$, a contradiction. The N-assignations that minimize J among $\mathcal{D}_N$ are uniform and as every uniform N-assignations have the same value by J, we obtain: the N-assignations that minimize J among $\mathcal{D}_N$ are the uniform N-assignations.

As $A_{\mathcal{G}_0}$ is uniform, we have: $J(\mathcal{G}_0) = J(d^*_{N_0})$ and

$$\forall \mathcal{G} : J(\mathcal{G}) \geq J(\mathcal{G}_0) \,.$$

□

The above optimality condition is necessarily limited to cases where B is relatively small. Indeed, as mentioned above, in a uniform graph, the cardinal of the intersection of any two blocks belongs to the set $\{\mu, \mu+1\}$ or $\{\mu\}$. But a consequence of Theorem 3 of [4] is that any such family of sets has a cardinal less than $\binom{V}{2}$ in the first alternative, and V in the second one. See Section 5.3.2 for an application of this result.

5.3 Solved Cases

We provide in this section three families of graphs which solve the MINVAR problem. The first family solves the case $K = 2$ (and the case $K = V - 2$, thanks to Proposition 3), the second one concerns configurations, and the third one Steiner systems.

5.3.1 Case $K = 2$

The the MINVAR problem can be solved for $K = 2$. The construction uses the notion of RRT (Round-Robin Tournament) which we define in Appendix A.

Theorem 2. *For $K = 2$, and any V, B, consider the graph $\mathcal{G}$ constructed with a RRT. Then $\mathcal{G}$ solves the MINVAR(B,V,K,γ) problem for any* $\gamma \geq 1$.

◇ *Proof* . Consider any graph $\mathcal{G}$. Using the Taylor expansion at $\gamma = 1$, we have (see Equation (13) in Section 3.2):

$$J(\mathcal{G}, \gamma) \;=\; (\gamma - 1)^2 \mu_2(\mathcal{G}) \;+\; (\gamma - 1) NI(\mathcal{G}) \;+\; B(B-1) \,.$$

Then, if we find a graph $\mathcal{G}'$ that minimizes $\mu_2(\mathcal{G})$ for all $\mathcal{G}$, and if this graph is also stable (*i.e.* it minimizes $NI(\mathcal{G})$), this graph will be optimal for all $\gamma \geq 1$.

Since $K = 2$, a graph $\mathcal{G}$ can be seen as a list of pairs of elements of $\mathcal{V}$. A RRT (Definition 10 in Appendix A) provides such a list $\mathcal{E}$ of $M = V(V-1)/2$ couples which are all distinct, according to Lemma 2.

Let $B = q \times M + r$, where q, r as the quotient and the remainder of the division of B by M. The list of blocks of $\mathcal{G}'$ is constructed as: q copies of $\mathcal{E}$, and one copy of the first r elements of $\mathcal{E}$. The graph $\mathcal{G}'$ constructed this way is stable in the sense of Definition 4, as a consequence of Lemma 3.

Now we prove that $\mathcal{G}'$ minimizes $\mu_2(\mathcal{G})$. By definition, $\mu_2(\mathcal{G})$ is the number of couples of $\mathcal{B}$-elements which have the same neighborhood. So, if we write $n_{(s,t)}$ the number of times that the couple (s,t) is used as neighborhood in $\mathcal{G}$, we obtain:

$$\begin{aligned} \mu_2(\mathcal{G}) &= \sum_{(s,t) \in C_2^V} n_{(s,t)}(n_{(s,t)} - 1) \\ &= \sum_{(s,t) \in C_2^V} n_{(s,t)}^2 - B \ . \end{aligned}$$

As the square function is convex and the sum of the $n_{(s,t)}$ is fixed, $a(\mathcal{G})$ is minimal if and only if the $n_{(s,t)}$ differ by at most one. This is precisely the case since in $\mathcal{G}'$, the $n_{(s,t)}$ are equal to q or $q+1$. This concludes the proof. □

5.3.2 Configurations and Quasi-Configurations

Configurations are structures such that blocks intersect at most on one point. Following [1, Chap. VI.7], we define:

Definition 9 (Configuration and Quasi-Configuration Graphs)**.** *A Configuration Graph is a graph $\mathcal{G}(\mathcal{B},\mathcal{V},\mathcal{E})$ such that: 1) $\forall b \in \mathcal{B}$, $|L(b)| = K$; 2) $\forall p \in \mathcal{V}$, $\delta(p) = r$; 3) $\forall b \neq b' \in \mathcal{B}$, $|L(b) \cap L(b')| \leq 1$.*

A Quasi-Configuration Graph is defined with 1), 3) and 2'): $\forall p \in \mathcal{V}$, $\delta(p) \in \{r, r+1\}$.

Quasi-Configuration graphs are, by definition, stable and uniform with $\mu = 0$. By application of Proposition 4, we have:

Corollary 1. *Quasi-Configuration graphs solve the MINVAR problem, for any $\gamma \geq 1$.*

Gropp, in Chapter VI.7 of [1] and references therein, provides lists of Configurations. We give now the construction of a family of Configurations.

Proposition 5. *Assume that $B = V$, that $\mathcal{B} = \mathcal{V} = [0..V-1]$ and $K \leq \log_2(V)$. Then the graph $\mathcal{G}$ defined as:*

$$L(b) = \{[b + (2^i - 1)] \ mod(V), i = 0..K-1\},$$

$b = [0..V-1]$, *is a Configuration. It therefore solves the MINVAR*(V,V,K,γ) *problem for any* $\gamma \geq 1$.

$\diamond$ *Proof* . In a first step, we prove that $\mathcal{G}$ is stable. Let us compute the degree of some $p \in \mathcal{V}$. Given the definition of $L(b)$, we have:

$$\forall p \in V, \quad L^{-1}(p) \;=\; \{[p-(2^i-1)]\; mod(V), i = 0..K-1\}\;.$$

But since $K \leq \log_2(V)$, each 2^i is smaller than V and the K values in this set are distinct. Therefore $|L^{-1}(p)| = K$ for all p and $\mathcal{G}$ is stable (it is actually r-regular).

In the second step, we prove that the blocks of $\mathcal{G}$ intersect at most once. Consider, without loss of generality, $0 \leq b < b' < V$. Then,

$$\begin{aligned} |L(b) \cap L(b')| &= |\{(i,i') \in \{0..K-1\}^2 \mid b+2^i-1 = [b'+2^{i'}-1] mod(V)\}| \\ &= |\{(i,i') \in \{0..K-1\}^2 \mid b'-b = [2^i-2^{i'}] mod(V)\}|\;. \end{aligned} \quad (22)$$

Then, two cases occur:

- either $b'-b < V/2$; since for every i, $2^i \leq V/2$ then $-V/2 \leq 2^i - 2^{i'} \leq V/2$. Then the “modulo” equality in (22) reduces to the arithmetic equality $2^i - 2^{i'} = b'-b$. Since $b \neq b'$, there is at most one solution to it, as a consequence of the uniqueness of the binary representation of integers.
- or $b'-b \geq V/2$; then the arithmetic equality is $V-(b'-b) = 2^{i'} - 2^i$. Again, since $V \neq b'-b$, there is at most one solution.

We conclude that in both cases, the set $L(b) \cap L(b')$ has cardinal 0 or 1. The graph is therefore uniform. By Proposition 4, the graph solves the MINVAR problem. □

5.3.3 Steiner Graphs

In this section, we prove that Steiner graphs (Definition 6) are solution to the MINVAR problem. To that end, we first calculate the interference function J for such graphs. We then use an extension of a result by Hobart[5] to prove that this function is actually a lower bound.

According to [6, Lemma 1], the number of blocks of a $S(t,K,V)$ Steiner system which contain a particular set of i points, $0 \leq i \leq t$, does not depend on the set in question, and is equal to:

$$\lambda_i \;=\; \frac{(V-i)!(K-t)!}{(V-t)!(K-i)!} \;=\; \binom{V-i}{K-i}\binom{V-t}{K-t}^{-1}\;. \quad (23)$$

In particular, $\lambda_0 = B$, see (19) and Definition 6. We extend the sequence λ_i with the definition: $\lambda_i = 1$, $t \leq i \leq K$.

The first result of this section is:

Theorem 3. *For a Steiner graph $\mathcal{G}$, there holds:*

$$J(\mathcal{G},\gamma) \;=\; B\sum_{\ell=0}^{K}(\gamma-1)^{\ell}\binom{K}{\ell}\lambda_\ell \;-\; B\gamma^K\,. \tag{24}$$

Proof. Let x_i denote the number of blocks of the Steiner system which intersect some block b at exactly i points. According to [7, 6], these values do not depend on the choice of the block b. Therefore, the numbers ν_ℓ defined in (10) can be written as $\nu_\ell = Bx_\ell$ and using the representation of $\widetilde{J}$ or J as a generating function (11), we have:

$$\widetilde{J}(\mathcal{G},\gamma) \;=\; B\sum_{\ell=0}^{K}x_\ell\gamma^\ell\,.$$

According to [7], the following general identity

$$\sum_{\ell=j}^{K}\binom{\ell}{j}x_\ell \;=\; \binom{K}{j}\lambda_j\,, \tag{25}$$

holds for any j, $0\le j\le t$. It turns out to be valid also for $t\le j\le K$, with the values $\lambda_j = 1$. Indeed, for $t<\ell<K$, x_ℓ is 0 and $x_K = 1$. The identity (25) reduces to $\binom{K}{j} = \binom{K}{j}\lambda_j$ in this case. Therefore, we have in general that:

$$\frac{1}{B}\,\widetilde{J}^{(j)}(\mathcal{G},1) \;=\; j!\sum_{\ell=j}^{K}\binom{\ell}{j}x_j \;=\; j!\binom{K}{j}\lambda_j\,.$$

Consequently, using Talyor's expansion of the polynomial $\widetilde{J}$ at $\gamma=1$, we simply obtain:

$$\widetilde{J}(\mathcal{G},\gamma) \;=\; B\sum_{\ell=0}^{K}(\gamma-1)^{\ell}\binom{K}{\ell}\lambda_\ell\,,$$

with Equation (24) as a consequence. □

In order to prove that Steiner graphs are optimal solutions for the MINVAR problem, we need to extend result of [5]. Let n_ℓ denotes the average number of blocks which have exactly ℓ element in common with some particular block. In other words and with our previous notation:

$$n_\ell \;=\; \frac{1}{B}\sum_{b\in\mathcal{B}}\left|b'\in\mathcal{B}\text{ s.t. }|L(b)\cap L(b')|=\ell\right| \;=\; \frac{\nu_\ell}{B}\,. \tag{26}$$

We shall also recall that $t-$designs are set systems such that each block have the same size, and each $t-$subset is contained in exactly λ blocks. When $\lambda=1$, this is the definition of Steiner systems.

Theorem 4. *For every graph $\mathcal{G}$ and for all $\ell\in\{0..K\}$:*

$$\sum_{t=0}^{K}\binom{t}{\ell}n_t \;\ge\; B\binom{K}{\ell}^2\binom{V}{\ell}^{-1} \tag{27}$$

with equality iff $\mathcal{G}$ is the graph of some ℓ-design. In addition,

$$\sum_{t=0}^{K} \binom{t}{\ell} n_t \geq \binom{K}{\ell} . \tag{28}$$

$\diamond$ *Proof* . The first inequality is Theorem 1 of [5]. For the second inequality, let $\lambda_{(p_1,..,p_\ell)}$ be the number of blocks containing the particular set $\{(p_1,..,p_\ell)\}$. It has been established in [5] that:

$$\begin{aligned} \sum_{(p_1,..,p_\ell)} \lambda_{(p_1,..,p_\ell)} &= B \binom{K}{\ell} \\ \sum_{(p_1,..,p_\ell)} (\lambda_{(p_1,..,p_\ell)})^2 &= B \sum_{t=0}^{K} \binom{t}{\ell} n_t . \end{aligned}$$

On the other hand, $\lambda^2 \geq \lambda$ for every integer λ. Consequently,

$$\sum_{t=0}^{K} \binom{t}{\ell} n_t = \frac{1}{B} \sum (\lambda_{(p_1,..,p_\ell)})^2 \geq \frac{1}{B} \sum \lambda_{(p_1,..,p_\ell)} = \binom{K}{\ell} .$$

This is (28). □

Now we can prove the main result of this section:

Theorem 5. *Assume a Steiner system $S(t,K,V)$ exists. Then the associated Steiner graph is a solution to the MINVAR (B,V,K,γ) problem (B given by* (20)*), for any $\gamma \geq 1$.*

$\diamond$ *Proof* . For every graph $\mathcal{G}$ we have, using the expansion at $\gamma = 1$ (13), the correspondences (14) and (26):

$$\widetilde{J}(\mathcal{G},\gamma) = B \sum_{\ell=0}^{K} \left(\sum_{t=0}^{K} \binom{t}{\ell} n_t \right) (\gamma-1)^\ell .$$

Now, fix some t and use inequality (27) for all $0 \leq \ell \leq t$ and (28) $t < \ell \leq K$. Then:

$$\widetilde{J}(\mathcal{G},\gamma) \geq B^2 \sum_{\ell=0}^{t} \binom{K}{\ell}^2 \binom{V}{\ell}^{-1} (\gamma-1)^\ell + B \sum_{\ell=t+1}^{K} \binom{K}{\ell} (\gamma-1)^\ell .$$

But according to the definition (23) of the numbers λ_i, and that of B: for all $0 \leq \ell \leq t$,

$$B \binom{K}{\ell} \binom{V}{\ell}^{-1} = \binom{V}{K} \binom{V-t}{K-t}^{-1} \binom{V-\ell}{K-\ell} \binom{V}{K}^{-1} = \lambda_\ell$$

and $\lambda_\ell = 1$ otherwise. So we obtain, using Theorem 3,

$$\widetilde{J}(\mathcal{G},\gamma) \;\geq\; B\sum_{\ell=0}^{K}\binom{K}{\ell}\lambda_\ell(\gamma-1)^\ell \;=\; \widetilde{J}(\mathcal{G}_{St},\gamma)\,,$$

where $\mathcal{G}_{St}$ is the Steiner graph with parameters (B,K,V), which exists by assumption. This graph is therefore optimal, independently of the value of $\gamma \geq 1$. □

6 Algebraic approach

Let $\mathcal{K} = \binom{\mathcal{V}}{K}$ be the set of subsets of $\mathcal{V}$ with cardinal K. Denote with $M = \binom{V}{K}$ the cardinal of $\mathcal{K}$. For two elements $\ell,\ell' \in \mathcal{K}$, let $I_{\ell\ell'} = \#(\ell\cap\ell')$. Finally, given a graph $\mathcal{G}$, and for each $\ell \in \mathcal{K}$ let n_ℓ be the number of elements of $b \in \mathcal{B}$ which are such that $L(b) = \ell$.

Using this notation, we have:

$$\begin{aligned}\widetilde{J}(\mathcal{G},\gamma) &= \sum_{\ell,\ell'\in\mathcal{K}}\;\sum_{b,b'|L(b)=\ell,L(b')=\ell'} \gamma^{I_{\ell\ell'}}\\ &= \sum_{\ell,\ell'\in\mathcal{K}} n_\ell n_{\ell'}\gamma^{I_{\ell\ell'}}\;.\end{aligned} \tag{29}$$

Denoting with $\mathbf{n}$ the (column) vector $(n_\ell)_{\ell\in\mathcal{K}}$ and with $\mathbf{A}(\gamma)$ the matrix with entries $\mathbf{A}(\gamma)_{\ell\ell'} = \gamma^{I_{\ell\ell'}}$, the value of $\widetilde{J}$ can be expressed as the quadratic form:

$$\widetilde{J}(\gamma) \;=\; \mathbf{n}'\,\mathbf{A}(\gamma)\,\mathbf{n}\,. \tag{30}$$

Accordingly, the problem MINVAR(B, V, K, γ) is equivalent to the combinatorial quadratic minimization problem:

$$\min_{\mathbf{n}\in N^M \text{ s.t. } |\mathbf{n}|=B} \mathbf{n}'\,\mathbf{A}(\gamma)\,\mathbf{n}\,.$$

Define next the function

$$\pi(\gamma) \;=\; \binom{V}{K}^{-1}\sum_{k=0}^{K}\binom{K}{k}\binom{V-K}{K-k}\gamma^k\,. \tag{31}$$

It is simple to see that

$$\mathbf{A}(\gamma)\mathbf{1} \;=\; M\,\pi(\gamma)\,\mathbf{1}\,. \tag{32}$$

where $\mathbf{1}$ is the vector of $\mathbb{R}^M$ which entries are all ones. This implies also:

$$\mathbf{1}'\mathbf{A}(\gamma)\mathbf{1} \;=\; M^2\,\pi(\gamma)\,. \tag{33}$$

The principal result of this section is the property:

Theorem 6. *For every $\gamma \geq 1$, the matrix $\mathbf{A}(\gamma)$ is definite positive.*

With the corollary:

Theorem 7. *For every bipartite graph $\mathcal{G}$ with $|\mathcal{B}| = B$, $|\mathcal{V}| = V$, and which satisfies Constraint* (9)*, we have:*

$$J(\mathcal{G},\gamma) \;\geq\; B^2\pi(\gamma) \;-\; B\gamma^K \;. \tag{34}$$

If $B = kM$ for some integer k, then the solutions are every design with exactly k copies of each element of $\mathcal{K}$, and equality holds in (34).

Another result is:

Theorem 8. *Assume that $B = kM + B'$ for some integers k and B'. Consider the set $\mathcal{S} = \{\boldsymbol{n} \in \mathbb{N}^M, |n| = B, \boldsymbol{n} \geq k\mathbf{1}\}$. Let $J_{B'}(\gamma)$ be the optimal value of MINVAR(B', V, K, γ). Then,*

$$\min_{\boldsymbol{n}\in\mathcal{S}} \boldsymbol{n}'\,\boldsymbol{A}(\gamma)\,\boldsymbol{n} \;=\; J_{B'}(\gamma) \;+\; (2B'kM + k^2M^2)\pi(\gamma) \;.$$

The proofs are provided in separate subsections.

It is important to observe that Theorem 8 does not imply that the MINVAR(B,V,K,γ) problem for $B > M$ can be reduced to a MINVAR problem for $B' \leq M$, because of the constraint on integer vectors in the set $\mathcal{S}$. See Proposition 9.

6.1 Proof of Theorem 6

For each $p = 0..K$, let A_p be the matrix:

$$(A_p)_{\ell,\ell'} \;=\; \begin{cases} 1 & \text{if } I_{\ell,\ell'} = p \\ 0 & \text{otherwise.} \end{cases}$$

With this new notation, the matrix $\mathbf{A}$ is:

$$\mathbf{A}(\gamma) \;=\; \sum_{p=0}^{K} \gamma^p A_p \;.$$

The family of matrices $(A_0,\ldots,A_K)$ is related with the *Johnson's Scheme* in the following way: $A_p = D_{K-p}$. It is known (see *e.g.* [3, chap. 21]) that the family $(D_0,\ldots,D_K)$ enjoys the following properties: $D_0 = Id$ and

- there exists a family of primitive, idempotent and symmetric matrices J_0, $\ldots J_K$ such that:

$$J_0 = \frac{1}{M}J, \qquad J_iJ_j = 0, \quad i \neq j \qquad \sum_i J_i = Id,$$

  where $J = \mathbf{1}\mathbf{1}'$ is the $M \times M$ matrix filled with ones.

- the following relationships hold:

$$J_k \;=\; \frac{1}{M}\sum_{i=0}^{K} q_k(i) D_i, \qquad D_k \;=\; \sum_{i=0}^{K} E_k(i) J_i,$$

where:

$$E_k(x) \;=\; \sum_{j=0}^{k} (-1)^j \binom{x}{j}\binom{K-x}{k-j}\binom{V-K-x}{k-j} \tag{35}$$

$$q_k(i) \;=\; E_i(k)\,\frac{V-2k+1}{V-k+1}\binom{V}{k}\binom{K}{i}^{-1}\binom{V-K}{i}^{-1}.$$

The functions $E_k(x)$ are *Eberlein polynomials*.

As a consequence, the matrix $\mathbf{A}(\gamma)$ can be expressed as:

$$\begin{aligned}
\mathbf{A}(\gamma) &= \sum_{\ell=0}^{K} \gamma^{\ell} A_{\ell} \;=\; \sum_{\ell=0}^{K} \gamma^{K-\ell} D_{\ell} \\
&= \sum_{i=0}^{K}\left(\sum_{\ell=0}^{K} \gamma^{K-\ell} E_{\ell}(i)\right) J_i \qquad (36)\\
&= \sum_{i=0}^{K}\left(\sum_{m=0}^{K} (\gamma-1)^m \sum_{\ell=0}^{K-m} \binom{K-\ell}{m} E_{\ell}(i)\right) J_i \\
&= \sum_{i=0}^{K}\left(\sum_{m=i}^{K} (\gamma-1)^m \binom{K-i}{K-m}\binom{V-m-i}{K-m}\right) J_i\,. \qquad (37)
\end{aligned}$$

The last equality follows from the insertion of the definition (35), and the identity proven in Lemma 4, Appendix C, with $Q = K-m$ and $R = V-K-i$. Let:

$$\varepsilon_i(u) \;=\; \sum_{m=i}^{K} u^m \binom{K-i}{K-m}\binom{V-m-i}{K-m}.$$

Then the projection of the matrix $\mathbf{A}(\gamma)$ onto the space generated by the matrices J_i writes as:

$$\mathbf{A}(\gamma) \;=\; \sum_{i=0}^{K} \varepsilon_i(\gamma-1)\, J_i\,.$$

Using the fact that the J_i are symmetric and idempotent, we have:

$$\begin{aligned}
\widetilde{J}(\gamma) &= \mathbf{n}'\,\mathbf{A}(\gamma)\,\mathbf{n} \;=\; \sum_{i=0}^{K} \varepsilon_i(\gamma-1)\,\mathbf{n}'\,J_i\,\mathbf{n} \\
&= \sum_{i=0}^{K} \varepsilon_i(\gamma-1)\,\mathbf{n}'\,J_i'\,J_i\,\mathbf{n} \\
&= \sum_{i=0}^{K} \varepsilon_i(\gamma-1)\,||J_i\,\mathbf{n}||^2 \;\geq\; 0
\end{aligned}$$

since, obviously, $\varepsilon_i(\gamma-1) \geq 0$ for all i and $\gamma \geq 1$. The matrix $\mathbf{A}(\gamma)$ is therefore positive definite.

6.2 Proof of Theorem 7

Consider the relaxed optimization problem:

$$\min_{\mathbf{x}\in R^M \text{ s.t. } |\mathbf{x}|=B} \mathbf{x}'\,\mathbf{A}(\gamma)\,\mathbf{x}\,.$$

Since the matrix $\mathbf{A}(\gamma)$ is positive definite, this is a convex optimization problem and the first-order solution to the Lagrangian are vectors $\mathbf{x}$ such that:

$$2\,\mathbf{A}(\gamma)\,\mathbf{x} \;=\; \lambda\,\mathbf{1}$$

where λ is the Lagrange multiplier of the constraint $|\mathbf{x}| = B$. It follows, see Equation (32), that $\mathbf{x} = (B/M)\mathbf{1}$ and $\lambda = 2M\pi(\gamma)$. When $k = B/M$ is an integer multiple of M, this solution belongs to $\mathbb{N}^M$. It is therefore the solution of the integer optimization problem. The value of the interference function is then obtained from $\widetilde{J}(\gamma) = (B/M)\mathbf{1}'\mathbf{A}(\gamma)(B/M)\mathbf{1} = (B/M)^2\mathbf{1}'\mathbf{A}(\gamma)\mathbf{1} = B^2\pi(\gamma)$ using (33).

6.3 Proof of Theorem 8

Assume that $\mathbf{n} = k\mathbf{1}+\mathbf{m}$. Then $|\mathbf{m}| = \mathbf{m}'\mathbf{1} = B'$, and we have:

$$\begin{aligned}
\mathbf{n}'\,\mathbf{A}(\gamma)\,\mathbf{n} &= k^2\,\mathbf{1}'\,\mathbf{A}(\gamma)\,\mathbf{1} \;+\; 2k\,\mathbf{m}'\,\mathbf{A}(\gamma)\,\mathbf{1} \;+\; \mathbf{m}'\,\mathbf{A}(\gamma)\,\mathbf{m} \\
&= k^2\,M^2\pi(\gamma) \;+\; 2kB'M\pi(\gamma) \;+\; \mathbf{m}'\,\mathbf{A}(\gamma)\,\mathbf{m}\,.
\end{aligned}$$

The result follows by minimization with respect to the vector $\mathbf{m}$ which is constrained to stay in the set $\mathcal{S}$.

7 Random Designs

In this section, we consider random graphs $\mathcal{G}$ generated by elementary methods, and we compute their performance criterion $J(\mathcal{G},\gamma)$, which is a random variable.

From a combinatorial perspective, it is interesting to see that the statistics of this random variable involve the function $\pi(\gamma)$ introduced in Section 6.

From the practical standpoint, it turns out that random graphs provide good approximations for some parameters.

7.1 Simple Random Designs

The simplest way to generate at random bipartite graphs (or designs) which satisfy the constraint (9) is, for each vertex b, to pick its neighborhood $L(b)$ uniformly at random among the $\binom{V}{K}$ possibilities. We call this method the "Simple Random Algorithm".

We show now that it is possible to compute the average value and the variance of the objective function for such randomly generated solutions. The key result for this is the distribution of the number of common points in two blocks.

Lemma 1. *Let $X_{bb'} = |L(b) \cap L(b')|$ be the interference number for each $b, b' \in \mathcal{B}$. Then:*

i) The distribution of $X_{bb'}$ is given by:

$$\mathbb{P}(X_{bb'} = k) \;=\; \binom{K}{k}\binom{V-K}{K-k}\binom{V}{K}^{-1} ;$$

ii) Its probability generating function is the function $\pi(\gamma)$ defined in (31)*, and it satisfies the identity:*

$$\begin{aligned} \pi(x) &= \binom{V}{K}^{-1} \sum_{k=0}^{K} \binom{K}{k}\binom{V-K}{K-k} x^k \\ &= \sum_{\ell=0}^{K} \binom{K}{\ell}^2 \binom{V}{\ell}^{-1} (x-1)^{\ell} ; \end{aligned} \tag{38}$$

iii) In particular, its first moment is $\mathbb{E}(X_{bb'}) \;=\; K^2/V$.

Proof. If k elements of $\mathcal{V}$ are common between $L(b)$ and $L(b')$, the set $L(b')$ is formed by adding $K-k$ elements chosen among the $V-K$ elements that are not in $L(b')$ (see the interpretation of the Chu-Vandermonde convolution in e.g. [8, p. 56]). This proves *i*).

The identity of *ii*) is proved in Appendix C.1. The result of *iii*) follows since $\mathbb{E}(X_{bb'}) = \pi'(1)$.

□

Using this notation, we have the following values for the first moments of the value of graphs generated by the Random algorithm.

Theorem 9. *If $\mathcal{G}$ is the graph generated by the Random algorithm, then*

$$\mathbb{E}(J(\mathcal{G},\gamma)) \;=\; B(B-1)\,\pi(\gamma) \tag{39}$$

$$\mathbb{V}(J^2(\mathcal{G},\gamma)) \;=\; 2B(B-1)\left(\pi(\gamma^2) - \pi^2(\gamma)\right) . \tag{40}$$

◇ *Proof* . If, with the notation of Lemma 1, $X_{bb'}$ is the cardinal of the intersection between blocks $L(b)$ and $L(b')$, then:

$$J(\mathcal{G},\gamma) \;=\; \sum_{b \neq b'} \gamma^{X_{bb'}} \qquad \widetilde{J}(\mathcal{G},\gamma) \;=\; \sum_{b,b'} \gamma^{X_{bb'}} .$$

Obviously, by the linearity of expectations, $\mathbb{E}[J(\mathcal{G},\gamma)] = B(B-1)\mathbb{E}(\gamma^X_{bb'}) = B(B-1)\pi(\gamma)$. Let us now compute the variance of $\widetilde{J}(\gamma)$. Results are easily extended to function J, which differs by the constant factor $B\gamma^K$.

We have:

$$\mathbb{V}(\widetilde{J}^2(\mathcal{G},\gamma)) \;=\; \sum_{b,b',c,c'} \operatorname{cov}\left(\gamma^{X_{bb'}}, \gamma^{X_{cc'}}\right) \;=\; \sum_{b,b',c,c'} \mathbb{E}\left(\gamma^{X_{bb'}+X_{cc'}}\right) \;-\; B^4\pi^2(\gamma) .$$

The value of the covariance depends on the number of distinct values in the quadruple (b, b', c, c'), as well as on their position. The enumeration of all cases is summarized in the following table. For this enumeration, the first column represents the type of configuration, with the convention that distinct letters represent distinct values of $[1..B]$, and that permutations of b/b', c/c', and $(b, b')/(c, c')$ are allowed.

Configuration	Number of Cases	$\mathbb{E}(\gamma^{X_{bb'}+X_{cc'}})$	Covariance
$(a,a;a,a)$	B	γ^{2K}	0
$(a,a;a,b)$	$4B(B-1)$	$\gamma^{K}\pi(\gamma)$	0
$(a,a;b,b)$	$B(B-1)$	γ^{2K}	0
$(a,b;a,b)$	$2B(B-1)$	$\pi(\gamma^2)$	$\pi(\gamma^2)-\pi^2(\gamma)$
$(a,a;b,c)$	$2B(B-1)(B-2)$	$\gamma^{K}\pi(\gamma)$	0
$(a,b;a,c)$	$4B(B-1)(B-2)$	$\pi^2(\gamma)$	0
$(a,b;c,d)$	$B(B-1)(B-2)(B-3)$	$\pi^2(\gamma)$	0

The only case which is not immediate is perhaps that of configuration $(a, b; a, c)$, since in this case $L(a) \cap L(b)$ and $L(a) \cap L(c)$ are not independent sets. However, *conditionally* on the value of $L(a)$, $L(a) \cap L(b)$ and $L(a) \cap L(c)$ are indeed independent subsets of $L(a)$. The cardinal of each is distributed according to $X_{bb'}$. Hence, the conditional distribution of $X_{ab} + X_{ac}$ has the distribution of the sum of two independent copies of this random variable, and since this does not depend on the particular value of $L(a)$, this is also true for the unconditional distribution.

Summing up the covariances for the different cases, we end up with the value:

$$\mathbb{V}(J(\gamma)) \;=\; \mathbb{V}(\widetilde{J}(\gamma)) \;=\; 2B(B-1)\left(\pi(\gamma^2) - \pi^2(\gamma)\right) \;,$$

which is (40). □

7.2 Filtered Random Algorithm

Another natural way to generate a random set system with B blocks is to choose B elements among the $M := \binom{V}{K}$ possible subsets of size K, uniformly. This result can be obtained by complementing the Simple Random algorithm with a *rejection* phase of subset already present in the list. This algorithm produces eventually B distinct blocks, on the obvious condition that $B \le M$. The distribution of the cardinal of the intersection between two blocks $L(b)$ and $L(b')$ becomes

$$\widehat{\pi}(x) \;=\; \mathbb{E}(x^{|L(b)\cap L(b')|}) \;=\; \frac{1}{M-1}\sum_{k=0}^{K-1}\binom{K}{k}\binom{V-K}{K-k}x^k \;=\; \frac{1}{M-1}(M\pi(x) - x^K)\;.$$

Accordingly, we obtain the:

Theorem 10. *If $\mathcal{G}$ is the graph generated by the Filtered Random algorithm, then*

$$\mathbb{E}(J(\mathcal{G},\gamma)) = B(B-1)\widehat{\pi}(\gamma) \quad (41)$$

$$\mathbb{V}(J^2(\mathcal{G},\gamma)) = 2B(B-1)\frac{(M-B)(M-B-1)}{(M-2)(M-3)}\left(\widehat{\pi}(\gamma^2)-\widehat{\pi}^2(\gamma)\right) . \quad (42)$$

◇ *Proof*. Again, with the notation of Lemma 1, $X_{bb'}$ is the cardinal of the intersection between blocks $L(b)$ and $L(b')$, then: $\mathbb{E}[J(\mathcal{G},\gamma)] = B(B-1)\widehat{\pi}(\gamma)$.

The computation for the variance also follows the same line as for Lemma 1, but the computations are more involved because there is no independence between the choice of blocks in the different situations. These computations are omitted. □

7.3 Other Variants of the Random Algorithm

A first modification of the Random algorithm is possible when $B \geq M$. In that case, $B = kM + B'$, with $B' < M$. Instead of picking B blocks at random, it is possible to pick k copies of each block, then pick at random the remaining B'. Using Equation (39) in Theorem 9 and the computation in the proof of Theorem 8, the performance of this algorithm is:

$$\mathbb{E}J(\mathcal{G},\gamma) = (B^2-B')\pi(\gamma) - (B-B')\gamma^K .$$

The difference with a graph $\mathcal{G}_R$ obtained with the unmodified Random algorithm is: $\mathbb{E}J(\mathcal{G},\gamma) = \mathbb{E}J(\mathcal{G}_R,\gamma) - (B-B')(\gamma^K - \pi(\gamma))$, which measures the improvement of this variant. The variance of the performance is reduced to $2B'(B'-1)\left(\pi(\gamma^2)-\pi^2(\gamma)\right)$.

Next, if we are convinced that it is possible to find a solution where $|L(b) \cap L(b')| \leq s$ for each $b, b' \in \mathcal{B}$, then we may improve the Simple Random algorithm by rejecting a block that has more than s vertices in common with the previous blocks. The Filtered Random algorithm is obtained for $s = K-1$. For smaller values of s, it is not clear that a new block can always be selected, or that it will be selected fast enough. Because of this, after some maximum number unsuccessful tries, we increase s to accept blocks more easily. This variant is discussed in [9].

8 Bounds

The purpose of this section is to discuss bounds (essentially, lower bounds) on the function $J(\mathcal{G},\gamma)$. These bounds can be used to test the optimality of some candidate solutions to the MINVAR(B,V,K,γ) problem. They can also be used to assess the performance of heuristics, through the computation of approximation ratios.

We have analyzed in Section 7 one family of heuristics: Random algorithms. Other algorithms, based on greedy choices or on round-robin constructions, have been empirically studied in [9]. It turns out that the Random algorithm actually provides, in general, better solutions with less computational effort.

8.1 Bounds from the Number of Interferences

The number of interferences can be used in bounds for the interference function as follows. We provide two upper and lower bounds: while the second ones are weaker, their expression is simpler and affine as a function of $NI(\mathcal{G})$.

Proposition 6. *For every bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, E)$ with $|\mathcal{B}| = B$ and $|\mathcal{V}| = V$ and such that $|L(b)| \leq K$ for all $b \in \mathcal{B}$, we have:*

$$B(B-1)\,\gamma^{\frac{NI(\mathcal{G})}{B(B-1)}} \;\leq\; J(\mathcal{G},\gamma) \;\leq\; B(B-1) \;+\; NI(\mathcal{G})\,\frac{\gamma^{\partial^o J(\mathcal{G},\gamma)}-1}{\partial^o J(\mathcal{G},\gamma)}\;. \tag{43}$$

This implies that:

$$B(B-1) \;+\; \log(\gamma) NI(\mathcal{G}) \;\leq\; J(\mathcal{G},\gamma) \;\leq\; B(B-1) \;+\; NI(\mathcal{G})\,\frac{\gamma^K-1}{K}\;. \tag{44}$$

Proof. The lower bound in (43) is obtained using the convexity of the power function $f(x) = \gamma^x$. Indeed:

$$\begin{aligned}
\frac{1}{B(B-1)} J(\mathcal{G},\gamma) &= \sum_{b\neq b'} \frac{1}{B(B-1)} f(|L(b)\cap L(b')|) \\
&\geq f\left(\sum_{b\neq b'} \frac{1}{B(B-1)} |L(b)\cap L(b')|\right) \\
&= f\left(\frac{NI(\mathcal{G})}{B(B-1)}\right).
\end{aligned}$$

The lower bound in (44) follows by bounding the convex function $f(x)$ below with its tangent at $x = 1$.

The upper bound in (43) results from the fact that if $0 \leq x \leq M$, and $\gamma \geq 1$, $\gamma^x \leq 1 + x(\gamma^M - 1)/M$. By the definition of the degree of J, every term $|L(b)\cap L(b')|$ is necessarily smaller than $\partial^o J$. The upper bound in (44) follows by bounding this degree by K: by assumption, $|L(b)\cap L(b')| \leq |L(b)| \leq K$ for all b, b'. □

Next, we provide a bound that depends solely on the parameters (B,V,K,γ). We use the fact that $NI(\mathcal{G})$ reaches its minimum when $\mathcal{G}$ is a stable graph. Let us denote the number of interferences $NI(\mathcal{G}_s)$ in a stable graph $\mathcal{G}_s$ with $I(B,V,K)$. It is given by, if $BK = Vr + q$:

$$I(B,V,K) := NI(\mathcal{G}_s) \;=\; q(r+1)^2 + (V-q)r^2 - BK \;=\; \frac{B^2K^2}{V} \;-\; BK \;+\; \frac{q(V-q)}{V}\;. \tag{45}$$

Using Proposition 6, we have:

Corollary 2. *For every B, K, V and γ, every bipartite graph $\mathcal{G} = (\mathcal{B}, \mathcal{V}, \mathcal{E})$ with $|\mathcal{B}| = B$ and $|\mathcal{V}| = V$ and which satisfies the constraint* (9)*, has the property:*

$$J(\mathcal{G},\gamma) \;\geq\; B(B-1)\,\gamma^{\dfrac{B^2K^2/V - BK + q(V-q)/V}{B(B-1)}}\;, \tag{46}$$

where $q = BK \bmod V$.

In the previous section, we have seen that the sum of the exponents in the formula defining $J(\mathcal{G},\gamma)$ is constrained: this sum is larger than that of a stable graph. This fact provides a new lower bound, obtained by relaxing the optimization problem.

Proposition 7. *For every bipartite graph $\mathcal{G} = (\mathcal{B},\mathcal{V},\mathcal{E})$ with $|\mathcal{B}| = B$ and $|\mathcal{V}| = V$ and such that $|L(b)| \leq K$ for all $b \in \mathcal{B}$, we have:*

$$J(\mathcal{G},\gamma) \;\geq\; r\times\gamma^{q+1} \;+\; (B(B-1)-r)\times\gamma^{q} \;, \tag{47}$$

where $I(B,V,K) = B(B-1)q + r$ with $r < B(B-1)$.

Proof. For a given graph, the list of values $|L(b)\cap L(b')|$ is a N-assignation (in the sense of Definition 8) for some $N \geq I(B,V,K)$, the latter quantity being defined in (45). Let $\mathcal{D}$ be the set of all such assignations. Among these assignations, let $\mathcal{D}_0$ be the set of $I(B,V,K)$-assignations.

Consider the set $\mathcal{C}$ of all N-assignations that are produced by some bipartite graph $\mathcal{G}$ with parameters B and V, such that $|L(b)| = K$ for all $b \in \mathcal{B}$. Obviously, $\mathcal{C} \subset \mathcal{D}$.

Then, for every bipartite graph with $|L(b)| = K$ for all $b \in \mathcal{B}$,

$$\begin{aligned} J(\mathcal{G},\gamma) &\geq \min_{(n_{bb'})\in\mathcal{C}} \sum_{b\neq b'} \gamma^{n_{bb'}} \\ &\geq \min_{(n_{bb'})\in\mathcal{D}} \sum_{b\neq b'} \gamma^{n_{bb'}} \\ &\geq \min_{(n_{bb'})\in\mathcal{D}_0} \sum_{b\neq b'} \gamma^{n_{bb'}} \;. \end{aligned} \tag{48}$$

The first inequality holds since obviously, $\mathcal{C} \subset \mathcal{D}$. The second one holds because from every N-assignation with $N \geq I(B,V,K)$, one can "extract" an $I(B,V,K)$-assignment which has a smaller value. The minimum in (48) is achieved for an assignation such that: if $I(B,V,K) = B(B-1)q + r$ with $r < B(B-1)$, r values are equal to $q+1$ and $B(B-1)-r$ values are equal to q. The value attained is then:

$$r\times\gamma^{q+1} \;+\; (B(B-1)-r)\times\gamma^{q} \;,$$

hence the result. □

Observe that the bound (47) is actually an improvement on (46). Denoting $\tau = B(B-1)$ and using convexity,

$$\frac{r}{\tau}\times\gamma^{q+1} \;+\; (1-\frac{r}{\tau})\times\gamma^{q} \;\leq\; \gamma^{\frac{r(q+1)+(1-r)q}{\tau}} \;=\; \gamma^{\frac{I(B,V,K)}{\tau}} \;.$$

Finally, observe that the bound (47) is reached if $\mathcal{G}$ is a stable and uniform graph. In that case, the graph solves the MINVAR problem and the bound is actually $J(\mathcal{G})$.

8.2 Bounds from Design Theory

The analysis of Section 5.3.3 and Section 6 has provided general bounds.

In particular, we have:

Corollary 3. *Given V and K and $M := \binom{V}{K}$, define for $0 \le \ell \le K$:*

$$B_\ell \;:=\; \binom{V}{\ell}\binom{K}{\ell}^{-1} \;=\; M\binom{V-\ell}{K-\ell}^{-1} .$$

Let then:

$$\ell^* \;=\; \max\{\ell \in [0..K] \mid B \ge B_\ell\} \;.$$

For every bipartite graph $\mathcal{G}$ with $|\mathcal{B}| = B$, $|\mathcal{V}| = V$, and which satisfies Constraint (9)*, we have:*

$$J(\mathcal{G},\gamma) \;\ge\; B\sum_{\ell=0}^{\ell^*}\binom{K}{\ell}\left\{\frac{B}{B_\ell}-1\right\}(\gamma-1)^\ell \,, \tag{49}$$

and the bound is attained for Steiner graphs. This bound is strictly better than (34) *of Theorem 7.*

Proof. From the proof of Theorem 5, we have, for each $t \in [0..K]$:

$$\widetilde{J}(\mathcal{G},\gamma) \;\ge\; B^2\sum_{\ell=0}^{t}\binom{K}{\ell}^2\binom{V}{\ell}^{-1}(\gamma-1)^\ell + B\sum_{\ell=t+1}^{K}\binom{K}{\ell}(\gamma-1)^\ell \,. \tag{50}$$

Using the facts that $\sum_{\ell=0}^{K}\binom{K}{\ell}(\gamma-1)^\ell = \gamma^K$, and $\widetilde{J} = J+\gamma^K$, this can be rewritten as:

$$J(\mathcal{G},\gamma) \;\ge\; B\sum_{\ell=0}^{t}\binom{K}{\ell}\left\{B\binom{K}{\ell}\binom{V}{\ell}^{-1}-1\right\}(\gamma-1)^\ell \,.$$

The term inside braces is positive as long as $\ell \le \ell^*$. Therefore, as ℓ increases from 0, the right-hand side provides an increasing sequence of lower bounds, which is maximal at $\ell = \ell^*$. The fact that the bound is attained by Steiner graphs is a consequence of Theorem 5.

Finally, to prove that (34) is not better, consider the identity (38). Since (34) is equivalent to $\widetilde{J}(\mathcal{G},\gamma) \ge \pi(\gamma)$, we find that (34) is actually a particular case of (50) for $t = K$. □

9 Conjecture

Every time we have been able to solve the MINVAR problem, we have observed that the solution does not depend on γ. We conjecture that this is always the case, and we explore in this section the implications of this conjecture.

Conjecture 1. *For every B, V, K, there is a graph $\mathcal{G}^*$ such that $\mathcal{G}^*$ is optimal for MINVAR(B, V, K, γ), $\forall \gamma \geq 1$.*

We know that uniform stable graphs and Steiner graphs do satisfy this property. Optimal graphs obtained with Theorems 2 and 5, of Corollary 1 in Section 5, all have this property. The exhaustive enumerations we have performed (reported in Appendix B.2), also have this property.

We propose two sets of results associated with this conjecture. The first one can be seen as different ways of stating it. The second one is about simpler, practical consequences. We have:

Proposition 8. *Assume that Conjecture 1 holds. Then it is also true that:*

i) If $\mathcal{G}$ is an optimal solution of MINVAR(B, V, K, γ) for $K+1$ distinct values of $\gamma \geq 1$, then $\mathcal{G}$ is optimal for MINVAR(B, V, K, γ), $\forall \gamma \geq 1$.

ii) Define $f_i(\mathcal{G}) = \sum_{b \neq b'} |L(b) \cap L(b')|^i$. If $\mathcal{G}^*$ is an optimal solution of MINVAR, then for all $i = 1..K$, $\mathcal{G}^*$ minimizes f_i among the graphs that minimize $f_1, \ldots, f_{i-1}$, under the constraint (9).

$\diamond$ *Proof*. Proof of i). If $\mathcal{G}$ is an optimal solution of MINVAR(B, V, K, γ) for $\gamma = \gamma_0, .., \gamma_K$, and $\mathcal{G}^*$ an optimal solution of MINVAR(B, V, K, γ), $\forall \gamma \geq 1$. We have $J(\mathcal{G}, \gamma_i) = J(\mathcal{G}^*, \gamma_i)$, $\forall i = 0..K$.

As $J(\mathcal{G}, \gamma)$ and $J(\mathcal{G}^*, \gamma)$ are γ-polynomials with a degree of at most K, $J(\mathcal{G}, \gamma) = J(\mathcal{G}^*, \gamma)$, $\forall \gamma$. In particular, $\mathcal{G}$ is optimal for all $\gamma \geq 1$.

Proof of ii). From Section 3.2, we have:

$$J(\mathcal{G}, \gamma) = B(B-1) + \sum_{i=1}^{K} \mu_i(\mathcal{G})(\gamma - 1)^i \tag{51}$$

where

$$\mu_p(\mathcal{G}) = \frac{1}{p!} \frac{\partial^p J}{\partial \gamma^p}(\mathcal{G}, 1) = \sum_{b \neq b' \in \mathcal{B}} \binom{|L(b) \cap L(b')|}{p}.$$

Since the factorial moments of the $|L(b) \cap L(b')|$ are related to the direct moments f_k through Stirling numbers of the first kind, we can write for each ℓ:

$$\mu_\ell(\mathcal{G}) = \sum_{1 \leq k \leq \ell} \frac{s(\ell, k)}{\ell!} f_k(\mathcal{G}), \tag{52}$$

where the numbers $s(\ell, k)$ do not depend on $\mathcal{G}$. Among those, $s(\ell, \ell) = 1$.

Assume now, by contradiction, that the statement is not true so that there exist values $k \in \{1..K\}$ such that some $\mathcal{G}^*$ does not minimize f_k among the graphs that minimize $f_1, \ldots, f_{k-1}$. Set j be the smallest one. It is characterized by:

$$\exists \mathcal{G}, \quad f_j(\mathcal{G}) < f_j(\mathcal{G}^*) \quad \text{and} \quad \forall i < j,\ f_i(\mathcal{G}) = f_i(\mathcal{G}^*),$$

and the last statement implies $\mu_i(\mathcal{G}) = \mu_i(\mathcal{G}^*)$ for all $i < j$, in view of (52). Using (51), we obtain that this graph $\mathcal{G}$ is such that when $\gamma \to 1^+$,

$$J(\mathcal{G},\gamma) - J(\mathcal{G}^*,\gamma) = \frac{f_j(\mathcal{G}) - f_j(\mathcal{G}^*)}{j!}(\gamma-1)^j + o((\gamma-1)^j) \ .$$

Since $f_j(\mathcal{G}) - f_j(\mathcal{G}^*) < 0$, $J(\mathcal{G},\gamma)$ is smaller than $J(\mathcal{G}^*,\gamma)$ when γ is sufficiently close to 1 which is in contradiction with the fact that $\mathcal{G}^*$ is optimal for all γ. Therefore, no such j exist, and $\forall i = 1..K$: $\mathcal{G}^*$ minimize f_i among the graphs that minimize $f_1, \ldots, f_{i-1}$. □

Both the results are based on the fact that, under Conjecture 1, the solutions to MINVAR would be characterized by a polynomial of degree K, and that such a polynomial is itself characterized by $K+1$ values, or $K+1$ derivatives (or possibly a mix of the two). Since the value of the polynomial at $\gamma = 1$ is already known, this actually reduces to K values or derivatives.

A possible practical use of this Proposition would be that the computation of the optimal polynomial can be done by solving K problems: either with different values using *i*), or sequentially using *ii*). In the second case, the objective functions to be minimized do not involve the parameter γ, and have certainly a strong combinatorial interpretation. For instance, *ii*) applied to $i = 1$ tells that all optimal graphs would all solve the MINNI problem, so that a search can be restricted to this class.

Observe also that the claim is *not* that $\mathcal{G}^*$ minimizes all functions $f_i(\cdot)$.

Next, we have:

Proposition 9. *Assume that Conjecture 1 holds. Then it is also true that:*

i) *If $\mathcal{G}^*$ is an optimal solution of MINVAR(B,V,K,γ), it minimizes the degree of $J(\mathcal{G})$, and among the graphs which have this property, it minimizes the leading term.*

ii) *Let $M := \binom{V}{K}$ and $d = \lfloor B/M \rfloor$. Each K-subset of $\mathcal{V}$ appears d times or $d+1$ times as a block.*

iii) *If $\mathcal{G}$ is an optimal solution of MINVAR(B,V,K,γ) for some $B < M := \binom{V}{K}$, then a solution to MINVAR$(M-B,V,K,\gamma)$ is obtained by selecting exactly the blocks not present in $\mathcal{G}$.*

◇ *Proof* . Proof of *i*). The value of $J(\mathcal{G},\gamma)$ can be expanded as $J(\mathcal{G},\gamma) = a\gamma^d + o(\gamma^d)$ $(\gamma \to \infty)$ with $a > 0$. Assume that there exists some graph $\mathcal{G}'$ such that $J(\mathcal{G}',\gamma) = a'\gamma^{d'} + o(\gamma^{d'})$, with either $d' > d$, or $d' = d$ and $a' > a$. Then there exists some value γ_0 such that $J(\mathcal{G},\gamma_0) < J(\mathcal{G}',\gamma_0)$, which contradicts the fact that $\mathcal{G}$ minimizes J for all values of γ.

Proof of *ii*). Let, as in Section 6, n_i be number of times that block $i = 1..M$ is used in $\mathcal{G}^*$. We have $J(\mathcal{G}^*,\gamma) = (\sum_i n_i(n_i-1))\gamma^K + \hat{J}(\mathcal{G}^*,\gamma)$ where $\hat{J}(\mathcal{G}^*,\gamma)$ is a polynomial of degree $K-1$.

According to *i*), $\mathcal{G}^*$ minimizes the degree of J and the leading term. The coefficient of γ^K is therefore minimal (and possibly 0). Now given that $\sum_i n_i = B$, $\sum_i n_i(n_i-1)$ is minimized if and only if each K-uple of V appears d times or $d+1$ times, $d = \lfloor B/M \rfloor$, as a block.

Proof of *iii*). Let $M := \binom{V}{K}$, and let $\mathbf{n}$ be the vector defined as in Section 6. Applying *ii*), we find $d = 0$, so that $\mathbf{n}$ is actually a binary vector, or the indicator vector of the blocks selected for $\mathcal{G}$. Selecting the blocks not in $\mathcal{G}$ gives the new vector $\mathbf{m} = \mathbf{1} - \mathbf{n}$. According to the expression (30) and to (32), the value of J for the graph $\mathcal{G}$ and for its transformed graph $\mathcal{G}'$ are related by:

$$\begin{aligned} J(\mathcal{G}') &= (\mathbf{1}-\mathbf{n})'\mathbf{A}(\gamma)(\mathbf{1}-\mathbf{n}) \;=\; \mathbf{1A}(\gamma)\mathbf{1} \;-\; 2\mathbf{n}'\mathbf{A}(\gamma)\mathbf{1} \;+\; \mathbf{nA}(\gamma)\mathbf{n} \\ &= M(M-2B)\pi(\gamma) \;+\; J(\mathcal{G})\ . \end{aligned}$$

Therefore $J(\mathcal{G})$ and $J(\mathcal{G}')$ are minimized simultaneously.

□

If Conjecture 1 holds, Proposition 9 tells that the search for solutions to MIN-VAR can be restricted to cases where $B \leq M$: by *ii*), solutions to cases where $B = kM + B'$ can be constructed by picking k copies of each block, and joining them to the solution for B'. See Theorem 8 and also Section 7.3. The statement *ii*) tells also that, in the representation of Section 6, only binary sequences $\mathbf{n}$ may correspond to optimal solutions for $B \leq M$. The search can actually be restricted to $B \leq M/2$, by *iii*). The validity of Proposition 9 has been checked on the examples calculated in Appendix B.2.

10 Conclusion

Acknowledgment The authors are greatly indebted to Stéphan Thomassé and Jean-Claude Bermond for their hints, and insightful and stimulating discussions on tournaments and design theory.

References

[1] C.J. Colbourn and J.H. Dinitz, editors. *Handbook of Combinatorial Designs*. Chapman & Hall/CRC, 2nd edition, 2007.

[2] T. Betz, D. Jungnickel, and H. Lenz. *Design Theory*, volume I. Cambridge University Press, second edition, 1999.

[3] F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes*. North Holland, 1977.

[4] D.K. Ray-Chaudhuri and Wilson R.M. On t-designs. *Oaska J. Math*, 12:737–744, 1975.

[5] S.A. Hobart. A characterization of t-designs in terms of the inner distribution. *Europ. J. Combinatorics*, 10:445–448, 1989.

[6] B.H. Gross. Intersection triangles and block intersection numbers of Steiner systems. *Math. Z.*, 139, 1974.

[7] N.S. Mendelsohn. A theorem on Steiner systems. *Canadian J. Math.*, 22:1010–1015, 1970.

[8] D.E. Knuth. *The art of computer programming Vol. 1*. Addison-Wesley, 1973.

[9] A. E. Baert, V. Boudet, A. Jean-Marie, and X. Roche. Optimization of download times in a distributed VOD system. In *ICPP'08: The International Conference on Parallel Processing*, pages 173–180, Los Alamitos, CA, USA, 2008. IEEE Computer Society.

[10] J. Riordan. *Combinatorial Identities*. Wiley, 1968.

A Round Robin Tournaments

Let $M = V(V-1)/2$. Consider the following constructions, which are illustrated in Figures 1 and 2. The end result of the construction is a standard Balanced Round-Robin Tournament (see [1]), but the order in which the matches are scheduled is of importance in our analysis.

Definition 10 (Round-Robin Tournament, RRT)**.** *We define a RRT as the sequence* $S = (e_0, e_1, .., e_{M-1})$ *of* M *couples of elements of* $[0..V-1]$*, resulting from the following construction.*

If V *is even,* e_i *with* $i = q \times V/2 + r$ *and* $0 \leq r < V/2$*, is:*

- *if* $r = 0$*,* $e_i = (q, V-1)$*.*
- *if* $r > 0$*,* $e_i = (q-r, q+r)$ *mod* $(V-1)$*.*

If V *is odd.* e_i *with* $i = q \times V + r$ *and* $0 \leq r < V$*,* $\quad 0 \leq q < (V-1)/2$*, is:*

- *if* $r < \frac{V-1}{2}$*:* $e_i = (q-r, q+1+r)$ *mod* $(V-1)$
- *if* $r = \frac{V-1}{2}$*:* $e_i = (q, V-1)$
- *if* $r = \frac{V+1}{2}$*:* $e_i = (q + \frac{V-1}{2}, V-1)$
- *if* $r > \frac{V+1}{2}$*:* $e_i = (q - (r - \frac{V+1}{2}), q + (r - \frac{V+1}{2}))$ *mod* $(V-1)$*.*

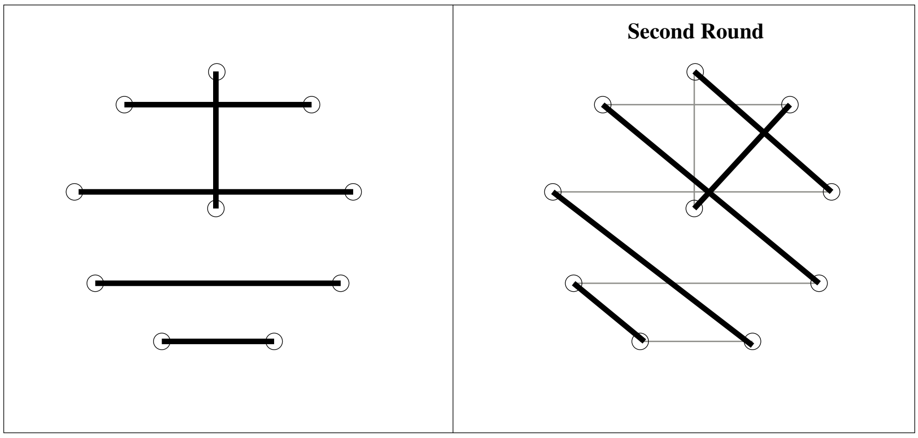

Figure 1: Construction of a RRT, case of even V

The construction for V even is visualized in Figure 1: a pairing of the V nodes is achieved in the first round (left), resulting in $V/2$ edges. Then the figure is rotated by $1/(V-1)$-th of a circle (right), and so on. For odd V, the construction of the first round is illustrated in Figure 2 (top and bottom-left), resulting in a cycle of V edges. The figure is then rotated by $1/(V-1)$-th of a circle (bottom-right), a maximum of $(V-1)/2$ times.

Definition 11. *A graph is called regular such that the degrees of vertices are d or $d+1$. A graph is called perfectly regular if all degrees are equal.*

Lemma 2. *Every RRT $(e_0, e_1, \dots, e_{M-1})$ is a permutation of the set of all couples (i, j), $i \neq j$.*

Proof. Let C_V^2 denote the set of all couples. Obviously, all the elements of $S = (e_0, e_1, .., e_{M-1})$ belong to C_V^2: we just have to prove that each element of C_V^2 is present in S. We do this by explicitly identifying the edge e in each case.

Consider first the case V even, and some $(s,t) \in C_V^2$, $s < t$:

- if $t = V-1$, then $(s,t) = e_{s \times V/2}$
- if $s+t$ is even: $(s,t) = e_{\frac{s+t}{2} \times V/2 + \frac{t-s}{2}}$
- if $s+t$ is odd:
  - if $\frac{s+t-1}{2} < \frac{V}{2}$: we have $(s,t) = e_{(\frac{s+t-1}{2} + \frac{V}{2}) \times V/2 + (\frac{V}{2} - \frac{t-s+1}{2})}$.
  - if $\frac{s+t-1}{2} \geq \frac{V}{2}$: we have $(s,t) = e_{(\frac{s+t+1}{2} - \frac{V}{2}) \times V/2 + (\frac{V}{2} - \frac{t-s+1}{2})}$

The couple (s,t) is therefore always in S.

Consider now the case where V is odd, and again $(s,t) \in C_V^2$, $s < t$:

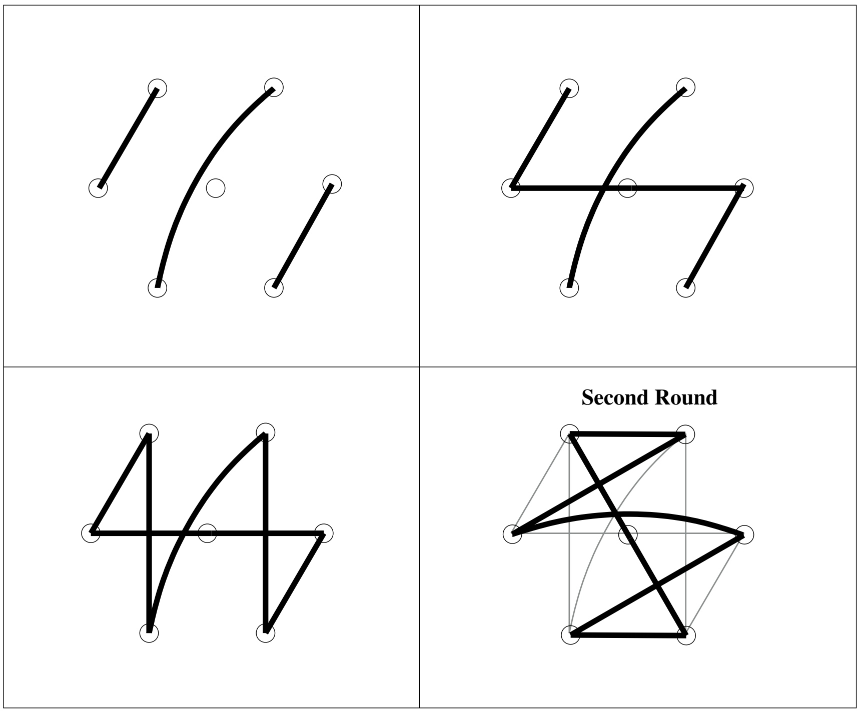

Figure 2: Construction of a RRT, case of odd V

- if $t = V - 1$:
  - if $s < \frac{V-1}{2}$: $(s,t) = e_{s\times V + \frac{V-1}{2}}$
  - if $s \geq \frac{V-1}{2}$: $(s,t) = e_{(s-\frac{V-1}{2})\times V + \frac{V+1}{2}}$
- if $t+s$ is odd:
  - if $\frac{t+s-1}{2} < \frac{V-1}{2}$: $(s,t) = e_{\frac{t+s-1}{2}\times V + \frac{t-s-1}{2}}$
  - if $\frac{t+s-1}{2} \geq \frac{V-1}{2}$: $(s,t) = e_{(\frac{t+s-1}{2}-\frac{V-1}{2})\times V + (\frac{V-1}{2}-\frac{t-s-1}{2})}$
- if $t+s$ is even:
  - if $\frac{t+s}{2} < \frac{V-1}{2}$: $(s,t) = e_{\frac{t+s}{2}\times V + (\frac{t-s}{2}+\frac{V+1}{2})}$
  - if $\frac{t+s}{2} \geq \frac{V-1}{2}$: $(s,t) = e_{(\frac{t+s}{2}-\frac{V-1}{2})\times V + (V-\frac{t-s}{2})}$

The couple (s,t) is therefore in S. □

Lemma 3. *Consider a RRT $(e_0, e_1, \ldots, e_{M-1})$. For every $i \in [0..M-1]$, the graph with vertices $[0..V-1]$ and edges $(e_0, e_1, \ldots, e_{i-1})$ is regular. If $V|i$, the graph is perfectly regular.*

Proof. With a slight abuse of notation, we shall speak of a "graph" for the sequence of its edges $(e_0, e_1, \ldots, e_{i-1})$. Lemma 2 implies that the graph constructed from these edges is a simple graph.

Consider first the case V even. By recurrence, we prove that $\forall q = 0..V-1$, $S_q = (e_0, e_1, .., e_{q\times V/2-1})$ is a perfectly regular graph and $\forall m < q \times V/2$, $(e_0, e_1, .., e_m)$ is a regular graph.

- For $q = 0$, the graph is empty and so perfectly regular.
- If these properties are valid for $q-1$, S_{q-1} is a perfectly regular graph. Now we prove that $(e_{q\times V/2}, .., e_{(q+1)\times V/2-1})$ contains exactly once each vertex: V vertices appear and for $p \in \mathcal{V}$: if $p = V$ or $p = q$, p appears in $e_{q\times V/2}$. Else there is $0 < i < V/2$ such as $p = [q+i]mod(V-1)$ or $p = [q-i]mod(V-1)$. Then, p appears in $e_{q\times V/2+i}$. So each vertex appear exactly once in $(e_{q\times V/2}, .., e_{(q+1)\times V/2-1})$, so the graph $(e_0, e_1, .., e_m)$ stays regular for $m \in q\times V/2, .., (q+1)\times V/2-1$ and S_q is perfectly regular.

Consider now the case where V is odd. By recurrence, we prove that $\forall q = 0..\frac{V-1}{2}-1$, $S_q = (e_0, e_1, .., e_{q\times V-1})$ is a perfectly regular graph and $\forall m < q \times V$, $(e_0, e_1, .., e_m)$ is a regular graph.

- For $q = 0$, the graph is empty and so perfectly regular.

t	K	V	B	$J(\mathcal{G},\gamma)$
5	8	24	759	$759\ (30+448\gamma^2+280\gamma^4)$
4	7	23	253	$253\ (112\gamma+140\gamma^3)$
3	6	22	77	$77\ (16+60\gamma^2)$
2	5	21	21	$21\ (20\gamma)$
5	6	12	132	$132\ (1+45\gamma^2+40\gamma^3+45\gamma^4)$
4	5	11	66	$66\ (15\gamma+20\gamma^2+30\gamma^3)$
3	4	10	30	$30\ (3+8\gamma+18\gamma^2)$
2	3	9	12	$12\ (2+9\gamma)$

Table 1: The polynomial J for graphs deduced from the Steiner systems $S(8,24,749)$ and $S(6,12,132)$

- If these properties are valid for $q-1$, S_{q-1} is a perfectly regular graph. So each vertex has exactly δ_{q-1} neighbors. As $(e_{(q-1)\times V},..,e_{(q-1)\times V+\frac{V-1}{2}-1}) = \{([q-i]mod(V-1),[q+1+i]mod(V-1))|i=0..\frac{V-1}{2}-1\}$, each vertex excepted $V-1$ appears exactly once: so $\forall m=0..(q-1)\times V+\frac{V-1}{2}-1$ we have $(e_0,e_1,..,e_m)$ is a regular graph. Moreover, in $(e_0,e_1,..,\ e_{(q-1)\times V+\frac{V-1}{2}-1})$ each vertex has $\delta_{q+1}+1$ neighbors except V which has δ_{q+1} neighbors.

  As $e_{(q-1)\times V+\frac{V-1}{2}} = (q,V)$ and $e_{(q-1)\times V+\frac{V+1}{2}} = ([q+\frac{V-1}{2}]mod(V-1),V)$ we have: $\forall m=0..(q-1)\times V+\frac{V+1}{2}$, $(e_0,e_1,..,e_m)$ is a regular graph and in $(e_0,e_1,..,\ e_{(q-1)\times V+\frac{V+1}{2}})$ each vertex has $\delta_{q+1}+1$ neighbors except $V,q,q+\frac{V-1}{2}$ which have $\delta_{q+1}+2$ neighbors.

  Finally as $(e_{(q-1)\times V+\frac{V+1}{2}+1},\ldots,e_{q\times V-1}) = \{([q-i]mod(V-1),[q+i]mod(V-1))|i=1..\frac{V-1}{2}-1\}$ each vertex appears exactly once except $V-1,q,q+\frac{V-1}{2}$ so $\forall m=0..q\times V-1$ we have $(e_0,e_1,..,e_m)$ is a regular graph and S_q is a perfectly regular graph.

$\square$

B Tables of Optimal Designs

B.1 Steiner Graphs

Steiner Graphs provide solutions to the MINVAR problem, according to Theorem 5. We list here some values of the interference function, obtained with formula (24).

The examples in Table 1 are obtained with the classical Steiner systems $S(8,24,749)$ and $S(6,12,132)$. Since Steiner systems $S(t-1,k-1,v-1)$ can be deduced from $S(t,k,v)$, the table includes the descending sequences as well.

Since there exist Steiner systems $S(2,3,6k+1)$ and $S(2,3,6k+3)$ for all values of k, Steiner graphs provide optimal solutions for $K=3$ when $B=6k^2+k$ or

$B = 6k^2 + 5k + 1$, respectively. The second entry in Table 1 with $t = 2$ belongs to this category. Projective planes $S(2, q+1, q^2+q+1)$, when they exist, provide optimal solutions for $K = q+1$ and $B = V = q^2+q+1$. The first entry in Table 1 with $t = 2$ belongs to this category.

B.2 More optimal designs

Through brute force enumeration, based on the algebraic approach, it is possible to find solutions to the MINVAR problem. We have implemented a program[6] which performs a systematic enumeration of the vectors $\mathbf{n}$ introduced in Section 6. For specified values of V, K and B, the program actually enumerates the set: $\{\mathbf{n} \in \mathbb{N}^M; |\mathbf{n}| = B, n_1 \geq n_i, i = 2..M\}$ where $M = \binom{V}{K}$, and computes the polynomial corresponding to each of them using (30). The constraint added on n_1 reduces the obvious redundancy obtained by permuting the elements of $\mathcal{V}$. The number of configurations tested by this method can be evaluated as the coefficient of z^B in the expression:

$$\sum_{t=1}^{B} z^t \left(\frac{1 - z^{t+1}}{1 - z} \right)^{M-1} .$$

Using this method for $V = 6$, $K = 3$ and $B \in [8..21]$, and $V = 7$, $K = 3$ and $B \in [4..14]$, we have obtained that there is indeed one polynomial which is uniformly smaller than any other. Tables 2 and 3 provide its value for $K = 3$, $V = 6$ or 7, and for $K = 4$, $V = 8$, respectively. The optimal value is denoted with $J_B(x)$, and the tables provide as well the transformed polynomial expanded at 1: $\widetilde{J_B}(x+1)$.

Some values in this table are provably optimal, as a consequence of Proposition 4: it can be checked that all polynomials listed in the tables satisfy: $J'_B(1) = I(B,V,K)$ where I is the minimal interference function defined in Equation (45). Equivalently, the coefficient of x in the modified polynomial $\widetilde{J_B}(x+1)$ is equal to $I(B,V,K) + BK$.

The graphs corresponding to these polynomials are therefore stable, see Proposition 1. The polynomials which have only two monomials of consecutive degrees correspond to graphs which are uniform in the sense of Definition 7. These graphs solve the MINVAR problem according to Proposition 4. These solutions are marked with an asterisk in Table 2. All rows but the last of Table 3 are instances of this result.

Among them, the solution for $K = 3$, $V = B = 7$ corresponds to the Fano Plane. The enumeration of graphs having the interference function $J(\mathcal{G}, \gamma) = 42\gamma$ shows that they are all isomorphic to this well-known design:

$$\{(123), (145), (167), (246), (257), (347), (356)\}$$

The optimal solution for $K = 3$, $V = 7$, $B = 6$ is obtained by removing any triple from the Fano Plane: such graphs are necessarily uniform. Removing a second triple breaks this property however.

[6] Available upon request.

	V	B	$J_B(x)$	$\widetilde{J_B}(x+1)$
	6	8	$18\,x^2+36\,x+2$	$8\,x^3+42\,x^2+96\,x+64$
*	6	9	$24\,x^2+48\,x$	$9\,x^3+51\,x^2+123\,x+81$
*	6	10	$30\,x^2+60\,x$	$10\,x^3+60\,x^2+150\,x+100$
	6	11	$42\,x^2+66\,x+2$	$11\,x^3+75\,x^2+183\,x+121$
	6	12	$54x^2+72x+6$	$12\,x^3+90\,x^2+216\,x+144$
	6	13	$66\,x^2+84\,x+6$	$13\,x^3+105\,x^2+255\,x+169$
	6	14	$78\,x^2+96\,x+8$	$14\,x^3+120\,x^2+294\,x+196$
	6	15	$94\,x^2+106\,x+10$	$15\,x^3+139\,x^2+339\,x+225$
	6	16	$108\,x^2+120\,x+12$	$16\,x^3+156\,x^2+384\,x+256$
	6	17	$126\,x^2+132\,x+14$	$17\,x^3+177\,x^2+435\,x+289$
	6	18	$144\,x^2+144\,x+18$	$18\,x^3+198\,x^2+486\,x+324$
	6	19	$162\,x^2+162\,x+18$	$19\,x^3+219\,x^2+543\,x+361$
	6	20	$180\,x^2+180\,x+20$	$20\,x^3+240\,x^2+600\,x+400$
	6	21	$2\,x^3+198\,x^2+198\,x+22$	$23\,x^3+267\,x^2+663\,x+441$
*	7	4	$10\,x+2$	$4\,x^3+12\,x^2+22\,x+16$
*	7	5	$18\,x+2$	$5\,x^3+15\,x^2+33\,x+25$
*	7	6	$30\,x$	$6\,x^3+18\,x^2+48\,x+36$
*	7	7	$42\,x$	$7\,x^3+21\,x^2+63\,x+49$
	7	8	$6\,x^2+48\,x+2$	$8\,x^3+30\,x^2+84\,x+64$
	7	9	$12\,x^2+54\,x+6$	$9\,x^3+39\,x^2+105\,x+81$
	7	10	$18\,x^2+64\,x+8$	$10\,x^3+48\,x^2+130\,x+100$
	7	11	$24\,x^2+76\,x+10$	$11\,x^3+57\,x^2+157\,x+121$
	7	12	$30\,x^2+90\,x+12$	$12\,x^3+66\,x^2+186\,x+144$
	7	13	$36\,x^2+108\,x+12$	$13\,x^3+75\,x^2+219\,x+169$
	7	14	$42\,x^2+126\,x+14$	$14\,x^3+84\,x^2+252\,x+196$
	7	15	$54\,x^2+138\,x+18$	$15\,x^3+99\,x^2+291\,x+225$
	7	16	$66\,x^2+150\,x+24$	$16\,x^3+114\,x^2+330\,x+256$
	7	17	$78\,x^2+166\,x+28$	$17\,x^3+129\,x^2+373\,x+289$
(1)	7	18	$90\,x^2+184\,x+32$	$18\,x^3+144\,x^2+418\,x+324$

Table 2: Table of optimal polynomials for $V=6$ or $V=7$, and $K=3$

Finally, the last row of Table 2, marked with a "(1)", results from an incomplete enumeration: only *binary* integer vectors have been tested. If Conjecture 9 is true, then we know from Proposition 9 *iii*) that the solution is indeed provided by such a vector.

V	B	$J_B(x)$	$\widetilde{J}_B(x+1)$
8	4	$4\,x^2+8\,x$	$4\,x^4+16\,x^3+28\,x^2+32\,x+16$
8	5	$12\,x^2+8\,x$	$5\,x^4+20\,x^3+42\,x^2+52\,x+25$
8	6	$18\,x^2+12\,x$	$6\,x^4+24\,x^3+54\,x^2+72\,x+36$
8	7	$30\,x^2+12\,x$	$7\,x^4+28\,x^3+72\,x^2+100\,x+49$
8	8	$40\,x^2+16\,x$	$8\,x^4+32\,x^3+88\,x^2+128\,x+64$
8	9	$56\,x^2+16\,x$	$9\,x^4+36\,x^3+110\,x^2+164\,x+81$
8	10	$72\,x^2+16\,x+2$	$10\,x^4+40\,x^3+132\,x^2+200\,x+100$

Table 3: Table of optimal polynomials for $V=8$ and $K=4$

C Combinatorial Identities

C.1 Identity in proof of Lemma 1

The identity to be proved is the equality between polynomials:

$$\binom{V}{K}^{-1}\sum_{k=0}^{K}\binom{K}{k}\binom{V-K}{K-k}x^k = \sum_{\ell=0}^{K}\binom{K}{\ell}^2\binom{V}{\ell}^{-1}(x-1)^\ell .$$

Expanding $x^k=(x-1+1)^k$ and identifying the coefficients of $(x-1)^\ell$, we have the equivalent identity: for all ℓ,

$$\binom{V}{K}^{-1}\sum_{k=\ell}^{K}\binom{k}{\ell}\binom{K}{k}\binom{V-K}{K-k} = \binom{K}{\ell}^2\binom{V}{\ell}^{-1} .$$

Expanding binomials, simplify and rearranging, we get successively:

$$\begin{aligned}
\sum_{k=\ell}^{K}\frac{(V-K)!}{(k-\ell)!(K-k)!^2(V-K-(K-k))!} &= \frac{(V-\ell)!}{(K-\ell)!^2(V-K)!}\\
\sum_{k=\ell}^{K}\frac{(V-K)!(K-\ell)!}{(k-\ell)!(K-k)!^2(V-K-(K-k))!} &= \binom{V-\ell}{K-\ell}\\
\sum_{k=0}^{K-\ell}\frac{(K-\ell)!}{k!(K-\ell-k)!}\,\frac{(V-K)!}{(K-\ell-k)!(V-K-(K-\ell-k))!} &= \binom{V-\ell}{K-\ell}\\
\sum_{k=0}^{K-\ell}\binom{K-\ell}{k}\binom{V-K}{K-\ell-k} &= \binom{V-\ell}{K-\ell} .
\end{aligned}$$

This last line is an instance of Vandermonde's convolution. The identity is therefore satisfied.

C.2 Identity in proof of Theorem 6

Lemma 4. *The following identity holds, for every $R, Q \geq 0$ and $m \geq i \geq 0$:*

$$\sum_{\ell=0}^{Q} \sum_{j=0}^{\ell} (-1)^j \binom{Q+m-\ell}{m} \binom{i}{j} \binom{Q+m-i}{\ell-j} \binom{R}{\ell-j} = \binom{Q+m-i}{Q} \binom{Q+R}{Q}. \tag{53}$$

Proof. The proof follows from the following series of rewritings. Let χ denote the left-hand side of (53). Then, swapping the summations and performing the change of variable $t = \ell - j$, we obtain:

$$\begin{aligned}
\chi &= \sum_{t=0}^{Q} \sum_{j=0}^{\ell} (-1)^j \binom{Q+m-t-j}{m} \binom{i}{j} \binom{Q+m-i}{t} \binom{R}{t} \\
&= \sum_{t=0}^{\infty} \binom{Q+m-t-i}{m-i} \binom{Q+m-i}{t} \binom{R}{t} \\
&= \sum_{t=0}^{\infty} \binom{Q+m-i-t}{m-i} \binom{Q+m-i}{Q+m-i-t} \binom{R}{t} \\
&= \sum_{t=0}^{\infty} \binom{Q+m-i}{m-i} \binom{Q}{t} \binom{R}{t} \\
&= \binom{Q+m-i}{Q} \binom{Q+R}{Q}.
\end{aligned}$$

In the second line, we use Identity (5a) of [10]:

$$\sum_{j \geq 0} (-1)^j \binom{n-j}{m} \binom{p}{j} = \binom{n-p}{n-m} = \binom{n-p}{m-p}.$$

The last line follows from Vandermonde's convolution. □

Contents

Centre de recherche INRIA Sophia Antipolis – Méditerranée
2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Grenoble – Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399